ACRONYMS AND TERMS

See the *IAFIS Acronym List and Glossary.*

✓ 226 p.

Department of Justice

Federal Bureau of Investigation

INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (IAFIS)

SYSTEM SPECIFICATION DOCUMENT

IAFIS-DOC-01090 -11.6

FINAL

August 27, 2008

Prepared By:

Federal Bureau of Investigation
Criminal Justice Information Services Division
1000 Custer Hollow Road
Clarksburg, WV 26306

NGI-262

This Page Intentionally Left Blank

CHANGE HISTORY SECTION

IAFIS-RS-0060(V01), August 15, 1995—This version incorporates RFCs 701, 793, 795, 803, 804, 808, 810, 812, 814, 818, 820, 821, 841, 842, and 900.

B. IAFIS-RS-0060(V2), October 24, 1995—This version incorporates RFC 693 (V1R1) two optional requirements moved from the non-mandatory section to the mandatory section; RFC 843 (V1R2) —ADP equipment, consoles, and cabinets height and depth requirement changed; RFC 854 (V1R2) —remove "non-mandatory" and "option" from requirements section and add Criminal Photo Function; RFC 871 (V1R2)—added new section concerning Noise Levels; RFC 890—IAFIS responses are grouped and printed for efficient output; RFC 892—clarified Fault Management Section; RFC 897—revised Traceability Matrix; RFC 909—all direct and indirect electronic communication eliminated between LCMS and IAFIS; RFC 917—allows DPS service providers to request RANRs or other reports.

C. IAFIS-RS-0060(V3), September 12, 1996—This version incorporates:
RFC 0870R2—Need to Define: a. the requirement for the service provider to cancel searches, b. the Latent Search Limit and how it will be implemented, c. and to develop overall resource utilization concept, specifications and flow requirements to segments
RFC 0904—To clarify the file comparison requirements in the III/FBI, AFIS/FBI, and ITN/FBI Segment Specifications.
RFC 0929—Replace "Process Control Number" with "IAFIS Control Number".
RFC 0938—To change the requirements supporting the handling and transmitting of electronic photos.
RFC 0939—Add paragraph about IAFIS Special Subject Filtering
RFC 0949R3—Changes for NCIC 2000 to IAFIS Recommended Interface For Changes For Wants and Flashes.
RFC 0955R1—To better explain the IAFIS Special Latent Cognizant Capabilities.
RFC 0995—Administrative changes to paragraphs 4.3.1.2, 4.3.1.3, 4.3.2 and 4.4.1. These changes are recommendations from Lockheed-Martin due to ECP03 re-plan effort.

D. IAFIS-RS-0060 (V4), June 6, 1997—This version release is a single sided document and will be managed as such hereafter, also incorporates the following RFCs:
RFC 961—Revised Table A-1 by adding sections 3.2.3.5.22 and 3.2.3.5.23 (Latent Processing Subelement Functions) and Sections 3.2.4.5.19 and 3.2.4.5.20 (Document Processing Subelement Functions) to the ITN/FBI PROC column.
RFC 998R1—Define MDD messages for Build E and related messages for Build F. Agreements for synchronized file updates.
RFC 1007—System-level requirements for document scanning eliminated to reflect program decisions which already deleted these requirements from ITN Segment Specification.
RFC 1048R1—Changes were made to correct system level documents to be consistent with III/FBI Segment Specification changes per RFC 992, Section 3.2.2.2.2. The changes listed in Section 9 above will match the III/FBI Segment Specification III-RS-0010 V5 baseline with negotiated ECP003 changes. This RFC is a delta to RFC 992 changes that were implemented based on requests recommended by the development contractor in conjunction with ECP003. These changes to the IAFIS System Specification and System Requirements Definition documents traced by RTM from changes to the III/FBI Segment Specification. A comparison

was made between the FBI's Version 5 of the III/FBI Segment Specification and the system documents. Finally, IDAS interfaces with III/FBI in the ICD no longer apply, based on first increment capabilities; those interfaces were deleted.
RFC 1025R2—During the review of the III/FBI Response Generation Software Design Document, it was suggested that Civil Response Generation only addresses responses from III/FBI searches of the Civil Subject Index Master File. Response Generation did not explicitly address the preparation of Identification and Non-Identifications resulting from the comparison of Civil fingerprint images as well as AFIS/FBI searches of the Civil On-line Features File.
RFC 1028—Wording changes needed to clarify requirements for test purposes. Deletion of 10 requirements that are neither testable nor required. Addition of 5 "shall" statements for test purposes. A combined SEU/LMIT effort to make the System Specification more responsive and eliminate non-testable requirements. This is the first of several RFCs that will pertain to and cause changes to the System Specification.
RFC 1032—Modify III/FBI Segment Specification and IAFIS System Specification to eliminate Transaction Status query for Ad Hoc Subject Searches, MRD Subject Searches, and Photo Requests. The design of the Ad-Hoc and IPS Functions provide for near instantaneous response. The MRD Functions will be maintained.
RFC 1041—Correct Subject Search Response time from 3 to 3.7 Seconds. ECP 03 changes the ITN Front End pass-through time for subject search from 200 ms to 900 ms, resulting in a subject search response time change from 3 sec to 3.7 sec. These corrections were made to Table 3-6 of the IAFIS System Specification, but the change in Response Time in Table 3-1 of the System Specification was overlooked. This RFC corrects Table 3-1 to make it consistent with previous ECP 03 changes.

E. IAFIS-RS-0060 (V5), August 20, 1997—This version release incorporates the following RFCs:
RFC1040R1—Revise affected documents to include country of citizenship (CTZ) as a descriptive field.
RFC1053R2—Vendors have requested more detail concerning the interface between NCIC 2000, IAFIS and the definition and allocation of the IAFIS message validation processing.
RFC1069R1—Removed non-mandatory requirements to service Criminal Photos in System Specification D.3.2, D.4.2, Table D-1, added additional key to processing photo requests in Section(s) 3.2.6.2 and 3.2.6.7b.
RFC1070R1—The changes in this RFC were necessary to conform to the modified concept for Unsolved Latent File operation across the IAFIS Segments.
RFC1078R1—Changes are necessary to conform to the modified concept of Latent Cognizant Queries.
RFC1089R1—Removed the language that referred to "minimum guaranteed searches".
RFC1098R1—To provide a File Comparison function which uses bitmaps to provide fast comparisons of the criminal and civil ten-print files.
RFC1099R1—Clarified External Image Request process, resolving inconsistencies and omissions in current message data definitions. Updated other messages returning images to maintain consistency.
RFC1101R1—This change provides the capability to search the manual civil files for unknown deceased, amnesia victims, missing persons, or submissions requesting a civil file search of the IAFIS files yields a non-ident.
RFC1106R1—Consistency with manual classification requirements, file name and deletion of design implementation requirement.
RFC1107R1—Training performance requirement "shall" modified to a "will". Deletion of data

entries upon expungement orders or record purge due to age limits clarified.
RFC1108—These changes remove the requirements for sealing fingerprint data in IAFIS.

F. IAFIS-RS-0060 (V6), December 22, 1997—This version release incorporates the following RFCs:
RFC1110R1—Consistency with text. Standard quality assurance practice.
RFC1111R1—Changed shall to will.
RFC1115R1—To clarify SLC operation, and existing requirements in IAFIS. documentation, and correct Build F MDD messages.
RFC1114R1—Added and deleted sections and subsections throughout Table A-1.
RFC1072R2—Requirements changes are necessary to reflect desired Want and Flash processing capability in IAFIS.
RFC1121R2—Deletion of MIDS. Revised User Fee Billing sections.
RFC1122R2—Deleted ICR, and added CSS information.
RFC1104R1—This change is to support the creation of contrived criminal records.
RFC1103R1—Modified to include requirements for ad hoc search.
RFC1134R1—Changes to include deletion, clarification, correction of requirements.
RFC1137R1—Changes to include an ident Fingerprint Image Submission (FIS) in the file update processes to the cert file.
RFC1146R1—Changes to include RTM requirement tags added to Section 3, for traceability to Table E.

G. IAFIS-RS-0060 (V7), February 11, 1998—Section 2, Applicable Documents, has been updated to include the latest versions of the Automated Fingerprint Identification System (AFIS/FBI) Segment Specification, Criminal Justice Information Services (CJIS) Technical Architecture, Identification Tasking & Networking (ITN/FBI) Segment Specification, Interstate Identification Index (III/FBI) Segment Specification, and the Integrated Automated Fingerprint Identification (IAFIS) System Requirements Definition (SRD). This version incorporates the following RFCs:
RFC1148R1—Requirements are applied to the appropriate segment(s) in Table 3-3. Made changes to "Category" as appropriate.
RFC1151R1—Standardization required to avoid ambiguities of interpretation between the System, ITN, AFIS, and III Segment Specifications. Deleted the Category A definition of availability. Renamed "Category B" availability to IAFIS Operational Availability.
RFC1157—Reconciles RTM identifiers.
Modifies Requirements: SS023100, SS034200(deleted a, b), SS036800a to SS036805, SS036800b to SS036810, SS039200(deleted a), SS039300a to SS039305, SS039300b to SS039310, SS039300c to SS039315, SS053100a to SS053105, SS053100b to SS053110, SS053100c to SS053115, SS056400a to SS056410, SS056400b to SS056420, SS060800(deleted b, a), SS062831a to SS062820, SS062831b to SS062825, SS062880a to SS062882, SS062880b to SS062884, SS071110a to SS071112, SS071110b to SS071114, SS071140a to SS071142, SS071140b to SS071144, SS076202b, to SS076203, SS076202c toSS076205, SS076226(deleted a), SS076228(deleted a), SS76226b to SS076227, SS076228b to SS076229, SS076234(deleted a), SS076234b to SS076235, SS076242(deleted a), SS076244a to SS076243, SS076244(deleted b), SS076244c to SS076245, SS076258(deleted a), SS076258b to SS076257, SS076272(deleted a), SS076274(deleted a), SS076647(deleted a), SS076647b to SS076649, SS077355(deleted a), SS077355b to SS077356.
Deletes Requirements: SS023000, SS029210, SS033515, SS036110, SS073320, SS079780, SS079785, SS079790, SS076272b, SS076274b, SS076648, SS076954, SS077356, SS077744,

NGI-266

SS082200, SS082250, SS082300, SS082206, SS082256, SS082306, SS082208, SS082258, SS082308, SS082210, SS082260, SS082310, SS023000, SS033515, SS036110, SS043290, SS050015, SS051120, SS051205, SS051210, SS073320, SS076272b, SS076274b, SS076648, SS076954, SS077356, SS077744, SS082200, SS082206, SS082208, SS082210, SS082250, SS082256, SS082258, SS082260, SS082300, SS082306, SS082308, SS082310, SS079780, SS079785, SS079790.
Adds Requirements: SS030150, SS031200, SS056400, SS062842, SS062843, SS056400.
RFC1164—These changes incorporate AOSS' comments into RFC1072R2. Requirements SS016774 added "and Flash" and deleted "from NCIC ($.A.WPT)". SS071120 was deleted. SS071150 added new text. SS071120 was deleted.

H. IAFIS-RS-0060 (V8), April 1, 1999—
This version release incorporates the following RFC:
RFC1199R2—Added SOR Requirements to Table 3-2, added NCIC 2000 SOR File to Figure 2, added new sections 3.1.3.6.12 and 3.1.3.9.1.9 with requirements. Updated the following tables to include SOR Requirements: 3-3, 3-5, A-1, E-1.

I. IAFIS-DOC-01090-9.0, August 22, 2005-

Document Number prefix was revised to reflect the current schema of CJIS document numbers. Also incorporated SPCR 21355k, which updated the IAFIS System Specification workload, response time, and traceability to support the IDENT/IAFIS V1.2.

CHANGE HISTORY PAGE

VERSION / REVISION	REVISION DATE	DESCRIPTION OF CHANGE	QA Approved	Date
V8R1	5-March-2002	NOTE: With this document revision, the CAO/CM/DMG assumes the administration of approved changes. The following SPCR(s) were incorporated: 12080a: The following waivers and deviations were incorporated by this SPCR: IAFISD0005 IAFISD0009 IAFISD0014 IAFISD0047 IAFISD0048 IAFISD0049 IAFISD0051 IAFISD0124 IAFISW0002 IAFISW0003 IAFISW0004 IAFISW0028 IAFISW0065 IAFISW0068 IAFISW0188 IAFISD0103—No accompanying documentation, therefore deviation is Closed. *NOTE:* "Figure 6 was changed to eliminate lines and arrows that should not have been there. There is no way to redline the drawing, as it is imported from visio." Quote from SPCR 12080a		
—	—	NOTE: This reflects SPCR 14886—Convert the IAFIS System Specification from WordPerfect to Word.	b6 b7C	
V8R2	10-February-2004	SPCR 17863b – Update Table 3-8a Criminal Ad Hoc Search Parameter Table and Table 3-8b Civil Ad Hoc Search Parameter Table in the IAFIS System Specification.		13 Feb 04
V9.0	22-August-2005	SPCR 21355k – Change doc number prefix and update workload, response time, and traceability.		9/19/2005

NGI-268

V10	04-October-2005	SPCR 17727W – Updated document to reflect changes made to support No Value Hops, as well as updates to tables to be consistent with SRD workload and response times and RequistePro Tags.		13 Dec 05
V10.1	06-February-2006	SPCR 23082b - Update to reflect changes to incorporate PI903 III Verify, Auto-Sequence Check, and Search But Don't Add. Update to reflect changes to remove Ten-Print MRD processing. Creation of unique requirement type & numbers with RequisitePro Application – requirements traceability tool.		23 May 06
V11.0	5/18/07	SPCR 25965 – This document incorporates the IAFIS System Specification, ITN, III, AFIS, IDWH, and EFCON Segment Specifications into one unified document. Comments received from CM incorporated. This reflects updates made to load IAFIS System Specification in RequisitePro, and link IAFIS SRD functional and non-functional requirements to system requirements. Grammatical and spelling edits also were made.		19 Jun 07
V11.1	08/14/2007	SPCR 27815b - reflects changes from 26510y (EMUF STOT)		16 Aug 07
V11.2	11/16/2007	This version reflects changes made to the format of the IAFIS System Specification to align with the IAFIS System Requirements Document. SPCR27519g - (DOCE) STOT		28 Nov 07
V11.3	01/17/2008	SPCR 29044a – Contains an IAFIS System Specification Reorganization to Reflect User Services.		11 Nov 08

V11.4	01/17/2008	SPCR 27871c – Added new requirements for cascaded ULF searches (Phase I). SPCR 27138d – Added new requirement. SPCR 27142h – Added new requirements for internal information requests. SPCR 28778b – Parent SPCR for the above SPCRs.	[redacted] b6 b7C	23 May 08
V11.5	6/23/08	SPCR 29558i – Added new requirements, etc. to incorporate iDSM.	[redacted]	05 Aug 08
V11.6	8/27/08	SPCR 28987b – Added new requirements to accept and store 1000ppi ten-print fingerprints. SPCR 30446a – Added Legacy Requirements that map to IAFIS SRD SPCR 30446b. SPCR 30113b – Parent SPCR ***Please note this document reflects the requirements baseline maintained in RequisitePro. ALL CHANGES MUST be made in RequisitePro, or changes will not be reflected in later versions of the document.*** ***Therefore, contact [redacted]@[redacted] for final version of the document if any changes or updates are made, including the CM signature box to the right for a final version for the CM document tree.***	[redacted] b6 b7C	09/08/08

NGI-270

This Page Left Intentionally Blank.

TABLE OF CONTENTS

NGI-274

LIST OF TABLES

This Page Left Intentionally Blank.

1 INTRODUCTION

The Criminal Justice Information Services (CJIS) Division is responsible for the operation and management of three vital criminal justice systems that provide information and data sharing services to the law enforcement community. These systems are the Integrated Automated Fingerprint Identification System (IAFIS), the National Crime Information Center (NCIC), and the National Instant Criminal Background Check System (NICS).

The IAFIS system provides law enforcement access to fingerprint identification and criminal history services. It also supports real time communications between systems by providing networking interfaces between international, federal, state, tribal, and local agency systems.

The NCIC system maintains a national index to documented theft reports, warrants and other criminal justice information submitted by law enforcement agencies from across the country. It provides law enforcement with access to criminal justice data pertaining to crimes and criminals of national interest.

The NICS system is a national system that provides authorized users with information about persons who may be prohibited by federal or state laws from owning or receiving a firearm.

Together, the systems comprise the CJIS System of Services (SoS), an integrated approach to providing customer information and services that support the detection and reduction of domestic and international terrorist and criminal related activities.

1.1 Purpose of Document

This document, the IAFIS System Specification, defines the functional and operational requirements for the system identified as the Integrated Automated Fingerprint Identification System. The requirements contained within this document reflect a decomposition of the requirements located in the IAFIS System Requirements Document (SRD). The purpose of this document is to bridge the user and functional requirements defined in the SRD to the system and segment level requirements detailed in the segment level design documents. To obtain a complete understanding of the IAFIS system requirements, this document should be used in conjunction with lower level IAFIS design documents (e.g., IAFIS ICD).

1.2 Background

The CJIS IAFIS, the largest fingerprint identification system in the world, has been instrumental in meeting the fingerprint identification needs of the law enforcement community. Since its inception in July 1999, IAFIS has provided automated ten-print and latent identification and criminal history data for both civil and criminal needs. Continuous improvements and upgrades since then have provided substantial increases in system performance, search reliability, throughput and response times.

1.3 System Objectives

IAFIS objectives are as follows:

- *Provide accurate and timely services to user agencies*: The FBI provides vital services to support law enforcement agencies and other users nationwide. To accomplish this mission, the FBI's automated systems must supply critical information in a timely manner.
- *Support a paperless environment*: Transactions received from and sent to other organizations, as well as internal FBI transactions, will be electronic to the maximum extent feasible. Since not all external organizations will be fully automated, some paper will be received for many years. Incoming fingerprint cards received in paper form will be converted to digital image form and processed electronically upon receipt.
- *Enable the FBI to process a significant growing workload without increasing staff*: The pressures on the federal budget dictate the use of high performance automation and work re-engineering to cope with increasing workloads.
- *Increase the number of crimes solved by providing enhanced identification and investigative services*: The improvement of both the Ten-Print and latent capabilities of IAFIS will assist law enforcement agencies in solving more crimes.
- *Provide options for IAFIS participation to international, federal, state, tribal and local agencies*: Each option will provide users with access to a different predefined level of IAFIS technical capability, so that each agency can choose the option best suited to its needs. Agencies may continue to mail Ten-Print cards and documents to the FBI for processing, or take full advantage of electronic data transmission and access a greater number of IAFIS capabilities.

1.4 Organization of Document

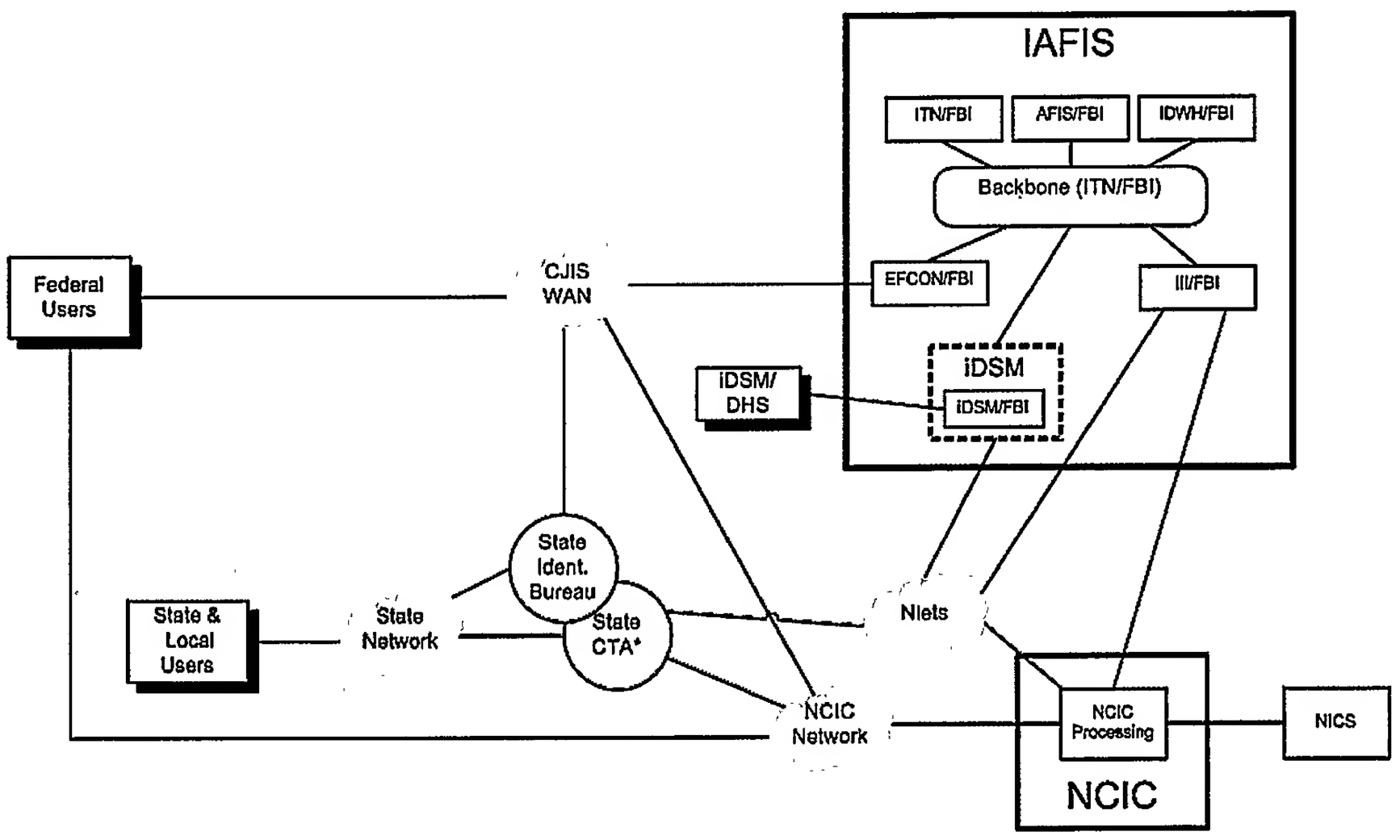
Following this introduction, Section 2 describes the exposed IAFIS User Service requirements, Section 3 describes the functional (system) requirements, and Section 4 contains a description of workload, performance, security, and other operational requirements. A bibliography is provided at the end of the document.

2 SYSTEM DEFINITION

2.1 IAFIS Segments

Six major segments make up the IAFIS: Identification Tasking and Networking (ITN), Interstate Identification Index (III), Automated Fingerprint Identification System (AFIS), Electronic Fingerprint Conversion (EFCON), the IAFIS Data Warehouse (IDWH), and the interim Data Sharing Model (iDSM). These segments work together to provide IAFIS services.

Figure 1 shows the IAFIS System Architecture. Electronic system transactions from local, state, and federal users are received and sent over the NCIC network and the CJIS Wide Area Network (WAN). Additional response communications with state systems occur using The International Justice and Public Safety Information Sharing Network (Nlets).



* The State CTA is responsible for control of all state commincations with the FBI
------ Denotes a prototype system

Figure 1. IAFIS System Architecture

2.1.1 EFCON Segment

The EFCON segment provides external communication services for IAFIS. EFCON supports access to the National Crime Information Center (NCIC) network, the NCIC front end, and the International Justice and Public Safety Information Sharing Network (Nlets).

EFCON manages the reception of electronic system transactions from external systems and users. EFCON receives and forwards fingerprint images and demographic data sent electronically to the

Federal Bureau of Investigation (FBI). EFCON accepts Electronic Fingerprint Transmission Specification (EFTS) transactions from state and federal agencies on the CJIS WAN, a private network administered by FBI personnel. EFCON validates, queues, forwards, and tracks electronic system transactions. EFCON is responsible for transferring the system transactions to the IAFIS ITN segment.

An external Card Scanning Service (CSS) provides a large volume scanning service for hardcopy fingerprint card submissions received by the CJIS Division. The CSS transmits scanned electronic fingerprint card submissions to IAFIS over a CJIS Wide Area Network.

2.1.2 ITN Segment

The ITN segment manages ten-print, latent fingerprint, document processing, and image retrieval services. The ITN segment also provides user Human-Machine Interfaces (HMIs), IAFIS internal communications, and supports networking and system management tasks.

2.1.2.1 ITN User Services

The ITN Ten-Print Processing Service (ITN/TPS) will provide ten-print workflow and workload management, HMIs, and the support services necessary to perform ten-print submission processing. The ITN/TPS area of responsibility will include the ten-print workstations and the software support for ten-print data entry, ten-print fingerprint image comparison, and the maintenance of fingerprint and criminal history files. ITN/TPS will accept, process, and respond to all service requests.

The ITN Latent Processing Service (ITN/LPS) will provide latent workflow and workload management, latent HMIs, and the latent support services necessary to perform latent fingerprint processing. The ITN/LPS area of responsibility will include latent workstations and software support for latent data entry, latent fingerprint classification, latent fingerprint comparison, and maintenance for latent fingerprint image and feature files.

The ITN Document Processing Service (ITN/DPS) will provide document workflow and workload management, document user interfaces, and the document support services necessary to perform document processing. The ITN/DPS area of responsibility will include document workstations and software support for document data entry, document supported maintenance of the criminal history files, and document generated reject or response generation.

The ITN Fingerprint Image Storage and Retrieval (ITN/ISRE) will provide the repository services for the storage and maintenance of digitized ten-print, latent fingerprint, and other fingerprint images. The ITN/ISRE area of responsibility will include providing image repository services that support the addition, retrieval, update, and deletion of image records.

2.1.2.2 ITN System Services

The ITN Backbone Communications Element (ITN/BCE) will provide internal communication services within IAFIS. ITN/BCE will support communication services within ITN and among IAFIS segments. ITN/BCE will provide connectivity between IAFIS segments, ITN elements, and ITN sub-elements.

The ITN segment will provide the connectivity between all IAFIS segments, in addition to the ITN segment communications requirements. ITN processing will convert hard copy and machine-readable data to an IAFIS input format through a combination of reading, scanning, and manual processing. ITN

NGI-281

will provide user interface and applications processing in support of ten-print, latent, and document services. ITN will perform storage, retrieval and file maintenance for fingerprint images.

- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Criminal Ten-print Fingerprint Image Master File.
- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Unsolved Latent Fingerprint Image File.
- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Latent Photo File.
- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Special Latent Cognizant Ten-print Image and Text File(s).
- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Major Case Print File.
- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Civil Ten-print On-line File.
- ITN/ISRE will be responsible for providing maintenance, storage, and retrieval for the Ten-print Certification File.

ITN will perform the following management functions:

- Manage ITN work group Service Provider assignments and maintain Service Provider status
- Manage ITN configuration and maintain system status
- Provide ITN backup and recovery
- Maintain a Transaction History
- Manage requests to/from other ITN sub-elements
- Manage requests to/from other ITN elements
- Manage requests to/from other IAFIS segment
- Collect performance data
- Send User Fee billing information to IDWHS

ITN will manage submissions from their point of entry into IAFIS and through completion of every processing function. Depending upon submission type, processing history, required completion time, processing still to be performed, and the current workload, ITN will allocate work to specific work groups and work group functions.

2.1.3 III Segment

The III segment provides five major user services:

- Subject Search
- Ad hoc Subject Search NGI-282

- File Maintenance
- Response Generation
- Criminal Photo Storage and Retrieval

Subject search uses a subject's name, physical characteristics, and biographic information to search the Subject Criminal History File. Subject search provides a list of the most likely candidates for identification. III will also store and retrieve criminal histories of subjects, or provide pointers to state files that contain the requested histories. The Interstate Photograph System (IPS) is an option, within III, that will provide storage and retrieval of criminal photos.

2.1.4 AFIS Segment

The AFIS segment provides the capability to perform fingerprint searches of the FBI's fingerprint repositories for potential matches to ten-print and latent fingerprint submissions. AFIS will provide a REJECT response to a fingerprint search. A candidate list that includes a list of the most likely candidates for identification or no candidates will be provided by AFIS in response to a fingerprint search. AFIS will provide the capability to manage ten-print and latent fingerprint searches. In addition, remote latent fingerprint search requests will be processed by AFIS.

2.1.5 IDWH Segment

The IDWH segment will collect, process, maintain, store, and archive data needed to support User Fee Billing (UFB). The IDWH services will be provided in a flexible and interactive environment so that required data can be reviewed and extracted as needed by appropriate FBI personnel. IDWH will consist of the following sub-elements;

- Transaction Status and Transaction History Sub-element (TS/THS)
- User Fee Billing Sub-element (UFBS)

The IDWH TS/THS will replicate the ITN historical transaction processing data to the UFBS. The ITN historical transaction processing data will consist of information needed to support identification, status, and location of ten-print and document transactions. The TS/THS database will provide the information for ITN to support Service Provider queries and report requests.

TS/THS will provide the IAFIS Service Providers access to the history records to locate, review, and reproduce the history records for specific transactions. TS/THS will provide access to the history records in order to generate statistical reports on IAFIS ten-print functions, document functions, and Service Provider performance and activity.

The FBI charges a fee for processing non-criminal, non-law-enforcement related fingerprint transactions. UFBS will collect, process, maintain, and store user fee fingerprint and name search transaction data furnished from the TS/THS and III. The user fee fingerprint and name search transaction data stored in UFBS are derived from III and ITN transaction processing data.

UFBS will receive, process, and store data related to IAFIS user fee fingerprint and name search transactions. UFBS will generate user fee bills and activity and revenue reports. UFBS will provide the capabilities to update bills and maintain user fee administrative data.

UFBS will generate hardcopy and softcopy billing reports for Federal and non-Federal central agencies; generate billing and direct payment activity reports for CJIS management; and generate softcopy Federal and non-Federal bills and revenue allocation reports for the FBI Finance Division. Authorized UFBS Service Providers will have the ability to modify billing rules, administrative data, and billing data as necessary.

2.1.6 iDSM Segment

The interim Data Sharing Model (iDSM) segment allows the FBI/CJIS and DHS/US-VISIT to efficiently and independently search a subset of fingerprint data from the other agency without increasing to the sharing agencies' search workload. The iDSM is implemented on an interim basis by making copies of one agency's fingerprint image data available at the other agency's location. The iDSM is comprised of the IAFIS Shared Want Files which contain IAFIS records and the DHS Shared Watch Files which contain IDENT records. In addition, the iDSM provides the ability to maintain the shared data in a timely manner.

2.2 Support System Users

IAFIS will support both indirect group users and direct individual users. Indirect group users are defined as users who request services without the use of system workstations or system terminals. IAFIS indirect group users are agencies that interact with IAFIS via the NCIC network, Nlets, NICS system, or other input media. Direct individual users are defined as users that are internal to IAFIS.

IAFIS will support two classifications of direct individual users: administrative users and Service Providers. The IAFIS administrative users are FBI personnel that support the IAFIS operations. These include System Administrator(s); System Security Administrator(s) (SSA); and Operations and Maintenance personnel.

The administrative users will access IAFIS services and data using IAFIS Service Provider Workstations (SPWs) or IAFIS consoles that are connected directly to IAFIS servers. The IAFIS Administrative users are CJIS support personnel who access the databases directly via command line or Human-Machine Interface (HMI). Administrator profiles will restrict data access and modifications based upon actual administration needs. Administrator profiles will include System Administrator (SA), System Security Administrator (SSA), and Data Base Administrators (DBA).

The IAFIS Service Providers are FBI personnel that support the basic IAFIS services provided to the federal, state, and local users. The IAFIS Service Providers perform activities that include data entry, fingerprint classification, fingerprint image comparison and verification, document processing, and latent fingerprint processing.

2.3 Process System Transactions

IAFIS will support user service requests by processing electronic system transactions. IAFIS defines system transactions as "the various types of input stimulants (electronic messages) that pass through IAFIS such as, fingerprint card submissions, documentation submissions, and subject search request

messages".

IAFIS will process electronic inter-segment system transactions. IAFIS defines inter-segment system transactions as "an electronic message request from one segment for a service provided by another segment, for example, subject search, fingerprint search, response generation".

IAFIS will process electronic intra-segment system transactions. IAFIS defines intra-segment system transactions as "an electronic message request from one element or sub-element of a segment to another element or sub-element requesting a service".

2.4 IAFIS User Services

The FBI provides user services to: (1) authorized customers located at law enforcement and criminal justice agencies, (2) others that have an authorized non-criminal justice purpose and (3) FBI staff members who are identified as Authorized FBI Service Providers.

There are six core IAFIS services to be provided to these users.

- The Identification Service provides a positive or negative identification of an individual based on a one-to-many biometric search.
- The Verification Service provides a confirmation of an identity based on a one-to-one comparison. This service is not currently supported by IAFIS.
- The Information Service supports user requests for biographic and/or biometric information for a specific individual.
- The Investigation Service provides a list of candidates based on a one-to-many biometric and/or biographic search. The result set may include an ordered listing of candidates and corresponding information to facilitate the investigative decision process.
- The Notification Service provides event notification to users. With this service, a data owner will receive an unsolicited notification from the system based on event criteria (triggers).
- The Data Management Service supports data management by providing authorized users the capability to add, delete, or modify biographic and/or criminal history data.

This Page Left Intentionally Blank.

3 SYSTEM FUNCTIONAL REQUIREMENTS

This section defines the functional requirements decomposed from the functional requirements contained within the IAFIS SRD. Section 3.1 through Section 3.6 contains the functional requirements specific to supporting the Core User Services. Section 3.7 provides the functional requirements relating to the internal IAFIS processes which provide the automated functions necessary to provide end-to-end transaction processing in support of the Core User Services. Section 3.8 contains the functional requirements relating to the specific areas of the administrative and control functions of IAFIS.

3.1 Identification Services Functional Requirements

The following sections contain the functional requirements supporting the IAFIS Identification User Services.

3.1.1 Ten-Print Fingerprint Identification Services

The Ten-Print Fingerprint Identification Services will provide the capability to match fingerprint information from criminal and civil Ten-Print submissions to fingerprint information contained within the IAFIS repositories. This service results in an identification decision (i.e., positive identification, non-identification). If the submission does not meet minimum processing criteria (e.g., quality), the submission will be returned with a reason for rejection. Ten-Print Fingerprint Identification Search requests submitted by Authorized Pilot Agencies will generate a search of the iDSM Shared Data independent of the IAFIS search.

SYS1 IAFIS (EFCON) shall provide Ten-Print Fingerprint Identification processing services for criminal ten-print submissions.

SYS2 IAFIS (EFCON) shall provide Ten-Print Fingerprint Identification processing services for civil ten-print submissions.

3.1.1.1 Ten-Print Fingerprint Identification Inputs

SYS3 IAFIS (EFCON) shall accept a Ten-Print Fingerprint Identification Search request via the CJIS WAN.

SYS4 IAFIS (EFCON) shall accept a Ten-Print Fingerprint Identification Search request via an IAFIS Workstation.

SYS5 IAFIS (EFCON) shall accept photo(s) as part of a Ten-Print Fingerprint Identification Search request.

IAFIS will accept photos which are compressed using the Joint Photographic Experts Group (JPEG) baseline sequential algorithm as specified in the EFTS.

SYS6 IAFIS (EFCON) shall accept rolled fingerprint images as part of a Ten-Print Fingerprint Identification Search request.

NGI-287

SYS7 IAFIS (EFCON) shall accept flat fingerprint images as part of a Ten-Print Fingerprint Identification Search request.

SYS2292 IAFIS (EFCON) shall accept fingerprint images at 1000 pixels per inch (ppi) from Authorized Contributors as part of a Ten-Print Fingerprint Identification Search request.

SYS8 IAFIS (EFCON) shall accept palm print images as part of a Ten-Print Fingerprint Identification Search request.

SYS9 IAFIS (EFCON) shall accept iris data as part of a Ten-Print Fingerprint Identification Search request.

3.1.1.2 Ten-Print Fingerprint Identification Processing

SYS10 IAFIS (ITN/TPS) shall process each Ten-Print Fingerprint Identification Search request using the assigned unique IAFIS Control Number (ICN).

SYS2293 IAFIS (EFCON) shall convert fingerprint images received at 1000ppi to 500ppi for processing as part of a Ten-Print Fingerprint Identification Search request.

SYS2294 IAFIS (EFCON) shall store all fingerprint images provided in 1000ppi format as part of a Ten-Print Fingerprint Identification Search request.

SYS2164 IAFIS (EFCON) shall initiate a Ten-Print Fingerprint Identification Search against the IDENT shared data as part of a Ten-Print Fingeprint Identification Search request from an Authorized iDSM Pilot Agency.

When an incoming Ten-Print Fingerprint Identification Search request or CPI Notification is from an Authorized iDSM Pilot Agency, IAFIS will search against the required repository but will also independently search and compare against the IDENT shared data in iDSM.

SYS2165 IAFIS (EFCON) shall send a Ten-Print Fingerprint Identification Search request to iDSM when the submitting agency is an Authorized iDSM Pilot Agency.

3.1.1.2.1 Quality Text Check

SYS11 IAFIS (ITN/TPS) shall perform an Automated Quality Check (AQC) of textual data (i.e., reason fingerprinted, arrest data) contained in a Ten-Print Fingerprint Identification Search Request against the AQC business rules.

AQC will verify that the submission textual data meets processing criteria for the TOT. If the AQC fails, the submission will be flagged for manual review or rejection.

SYS12 IAFIS (ITN/TPS) shall reject a Ten-Print Fingerprint Identification Search Request when textual information is invalid based on AQC business rules.

SYS13 IAFIS (ITN/TPS) shall require an Authorized FBI Service Provider to perform Manual Quality Check (QC) on a Ten-Print Fingerprint Identification Search Request when AQC business rules determine manual review is necessary.

SYS14 IAFIS (ITN/TPS) shall allow an authorized FBI Service Provider to reject a Ten-Print Fingerprint Identification Search Request when it is determined to be invalid as part of Manual QC.

NGI-288

3.1.1.2.2 Subject Search

SYS15 ITN/TPS shall initiate a Subject Search Request to III when the Ten-Print Fingerprint Identification Search request does not contain a supplied (quoted) FNU.

SYS16 IAFIS (III) shall search the criminal records in the IAFIS repository for candidates based on biographic data provided as part of Ten-Print Fingerprint Identification Search Request.

A civil Subject Search is only performed for missing person's transactions (i.e., MPR and IMPR Humanitarian TOTs).

SYS17 IAFIS (III) shall search the civil records in the IAFIS repository for candidates based on biographic data provided as part of a Humanitarian Ten-Print Fingerprint Identification Search Request when no identification is made to a criminal record.

3.1.1.2.3 Automated Fingerprint Sequence Check (ASC)

SYS18 IAFIS (ITN/TPS) shall set a Perform ASC flag to indicate whether a transaction is to undergo an ASC review.

SYS19 IAFIS (AFIS) shall process each Ten-Print Fingerprint Identification Search request through the Automated Fingerprint Sequence Check (ASC) function when the Perform ASC flag is set.

3.1.1.2.4 Automated Fingerprint Image Quality Check

SYS20 IAFIS (AFIS) shall perform an Automated Image Quality Check based on image quality standards when a Ten-Print Fingerprint Identification Search Request passes Automated Fingerprint Sequence Check.

SYS21 IAFIS (AFIS) shall automatically measure and record the quality of characteristics extracted for each finger used in the Ten-Print Fingerprint Identification Search request as part of the automated image quality check.

SYS22 IAFIS (AFIS) shall set the SBDA Flag when the quality value returned from a feature extraction is below the SBDA threshold value and greater than or equal to the feature search threshold.

SYS23 IAFIS (AFIS) shall reject a Ten-Print Fingerprint Identification Search Request when the fingerprint images fail to satisfy minimum fingerprint image quality standards.

Criteria used for determining the fingerprint image quality are included in the AFIS Software Design Document (SDD).

3.1.1.2.5 III/Verify

When an incoming submission references at least one FNU, a fingerprint comparison of each contributor supplied (quoted) FNU is made prior to a technical search and/or subject search.

SYS24 IAFIS (AFIS) shall perform a III/Verify service for each quoted FNU or Subject Search candidate on a Ten-Print Fingerprint Identification Search request.

SYS25 IAFIS (ITN/TPS) shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing

indicator (e.g., SPF) as part of a Ten-Print Identification Search request.

3.1.1.2.6 Manual Fingerprint Sequence Check (FSC)

SYS26 IAFIS (ITN/TPS) shall require an Authorized FBI Service Provider to perform Manual Fingerprint Sequence Check (FSC) on a Ten-Print Fingerprint Identification Search Request when ASC determines that manual review is necessary.

The Fingerprint Sequence Check is used to verify that fingerprint images within a ten-print submission are in the correct sequence. This is done to ensure the correct fingerprint images are used to search the IAFIS features files (e.g., Criminal Ten-print Features Master File).

SYS27 IAFIS (ITN/TPS) shall forward the Ten-Print Fingerprint Identification Search request to AFIS for further processing after a successful FSC review by the Authorized FBI Service Provider.

ITN will set the Perform_ASC flag to 'N', which causes AFIS to skip the ASC function and continue processing accordingly (e.g., Feature Search, III/Verify).

SYS28 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to reject a Ten-Print Fingerprint Identification Search Request as part of Manual FSC when fingerprint data fails to meet processing criteria.

3.1.1.2.7 Fingerprint Feature Search

SYS29 IAFIS (AFIS) shall perform a feature search of the criminal records in the IAFIS repository when a Ten-Print Fingerprint Identification Search Request does not contain candidate(s).

The criminal and civil Ten-Print submissions will be searched against the Criminal Ten-Print Fingerprint Features master file. Humanitarian submissions will be searched first against the criminal file. If no identification is made, Humanitarian submissions will then be searched against the civil file.

SYS30 IAFIS (AFIS) shall perform a feature search of the civil records in the IAFIS repository as part of a Humanitarian Ten-Print Fingerprint Identification Search Request when no identification is made to a criminal record.

SYS2166 IAFIS (iDSM) shall search the fingerprint features of the IDENT shared data records as part of a Ten-Print Fingerprint Identification search request submitted by an Authorized iDSM Pilot Agency.

SYS31 IAFIS (AFIS) shall provide a ranked candidate list with zero or more candidates as part of the Ten-Print Fingerprint Identification Search Request.

The AFIS feature search will return up to a configurable number of candidates to ITN for processing.

SYS2167 IAFIS (iDSM) shall determine a "match score" for each candidate resulting from a feature search of the IDENT shared data contained within iDSM.

SYS32 IAFIS (AFIS) shall automatically determine a positive identification decision for each candidate that has a match score above the high confidence threshold as part of a Ten-Print Identification Search Request.

Identification decisions may require manual Fingerprint Image Compare (FIC), depending on the match score. If the match score is above the high confidence threshold then no manual FIC is required. If the match score is below the high confidence threshold and above the low confidence threshold then one manual FIC is required to verify the identification decision returned by AFIS. If the match score is below the low confidence threshold then two FICs are required.

SYS33 IAFIS (AFIS) shall set the AFIS FIC Indicator according to the candidate match score.

SYS34 IAFIS (ITN/TPS) shall support three automated fingerprint identification review levels (AFIS FIC Routing Indicator).

SYS35 IAFIS (ITN/TPS) shall support an automated fingerprint identification review level that requires one manual FIC for a candidate match score below the high confidence threshold.

SYS36 IAFIS (ITN/TPS) shall support an automated fingerprint identification review level that requires two manual FICs for a candidate match score below the low confidence threshold.

SYS37 IAFIS (ITN/TPS) shall support an automated fingerprint identification review level that does not require a manual FIC for a candidate match score above the high confidence threshold.

3.1.1.2.8 Fingerprint Comparison

SYS38 IAFIS (ITN/TPS) shall perform a Ten-Print Fingerprint Comparison for each candidate contained in a Ten-Print Fingerprint Identification Search request.

iDSM manual image comparisons performed on candidates resulting from a search of the IDENT shared data records will be performed on IAFIS (ITN) workstations that are independent of normal IAFIS workflow.

SYS39 IAFIS (ITN/TPS) shall generate ITN/ISRE fingerprint image retrieval requests to support Ten-Print Fingerprint Comparison processing.

SYS40 IAFIS (ITN/TPS) shall route the submission to an error queue when images are not found in the FIMF during FIC processing.

SYS41 IAFIS (ITN/TPS) shall display the retrieved candidate images and the submission image for an Authorized FBI Service Provider to perform the Fingerprint Image Comparison (FIC) function.

SYS42 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to provide the decision for a Ten-Print Fingerprint Identification Search Request as a result of the manual FIC.

SYS43 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to reject a Ten-Print Fingerprint Identification Search Request as a result of the manual FIC.

SYS44 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request to a second FIC Service Provider when two manual FICs are required and the first FIC Service Provider returns an identification decision.

SYS45 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request for review by an EVAL Service Provider when the automated fingerprint identification review level requires two manual FICs, the candidate match score was above the EVAL threshold, and the first FIC Service Provider returns a non-identification decision.

SYS2161 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request

for review by an EVAL Service Provider when the automated fingerprint identification review level requires two manual FICs, the candidate match score was below the EVAL threshold, the candidate was produced from a positive name search, and the first FIC Service Provider returns a non-identification decision.

SYS46 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request for review by an EVAL Service Provider when one FIC Service Provider returns an identification decision, and a second FIC Service Provider returns a non-identification decision.

SYS47 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request for review by an EVAL Service Provider when one FIC Service Provider returns an identification decision, and a second FIC Service Provider returns a reject decision.

SYS48 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request for review by an EVAL Service Provider when the automated fingerprint identification review level requires a manual FIC and the FIC Service Provider returns a non-identification decision.

SYS49 IAFIS (ITN/TPS) shall forward a Ten-Print Fingerprint Identification Search request for review by an EVAL Service Provider when the automated fingerprint identification review level requires a manual FIC and the FIC Service Provider returns a reject decision.

SYS2168 IAFIS (iDSM) shall reject any search request of the IDENT shared data that has been determined "Unable to Process" by three independent manual image comparison service providers.

SYS50 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to replace any or all fingerprint images in the fingerprint composite image with the images provided in the Ten-Print Fingerprint Identification Search request when the FIC decision is a positive identification.

SYS51 IAFIS (ITN/TPS) shall forward the Ten-Print Fingerprint Identification Search request to the Criminal Consolidation Function when more than one criminal candidate receives an identification decision.

SYS2169 IAFIS (iDSM) shall require an Authorized FBI Service Provider to perform a Post Process Review check on all positive identifications resulting from a Ten-Print Fingerprint Identification Search of the IDENT shared data records.

3.1.1.2.9 Search But Don't Add

The Search But Don't Add (SBDA) flag allows Ten-Print submissions to search IAFIS repositories without allowing image and feature updates to IAFIS. Humanitarian prints will be added despite the SBDA flag being set. If the submitted prints result in a non-identification decision, IAFIS will respond with a quality reject message.

SYS52 IAFIS (ITN/TPS) shall process a Search but Don't Add (SBDA) type that allows a Ten-Print Fingerprint Identification Search request of a defined quality to search the criminal file, but not be added to the fingerprint image file.

SYS53 IAFIS (ITN/TPS) shall indicate to the Authorized FBI Service Providers that images of poorer quality will not be added to the fingerprint image database when candidates from an SBDA submission are provided for viewing on the IAFIS Workstation.

SYS54 IAFIS (ITN/TPS) shall reject the Ten-Print Fingerprint Identification Search request

when the SBDA indicator is set and the search results in a non-identification decision.

3.1.1.2.10 Certification File Maintenance

SYS55 IAFIS (ITN/TPS) shall create a copy of the Ten-Print Fingerprint Identification Search Request for the IAFIS Certification File based on file maintenance rules.

SYS56 IAFIS (ITN/TPS) shall store submissions in the Ten-print Certification File after processing is complete.

SYS57 IAFIS (ITN/TPS) shall store submission information in the Ten-print Certification File if a criminal retained ten-print submission is Non-IDENT.

SYS58 IAFIS (ITN/TPS) shall store submission information in the Ten-print Certification File if a ten-print submission is determined to be a positive identification against an existing criminal record.

SYS59 IAFIS (ITN/TPS) shall provide the location of the Ten-Print Certification File created to III for recording with event data.

3.1.1.2.11 LESC Shared Data Search

SYS2170 IAFIS (iDSM) shall send an IAQ to LESC, when the daily configured limit is not exceeded, for any positive identification resulting from a Ten-Print Fingerprint Identification Search of the IDENT shared data records.

SYS2171 IAFIS (iDSM) shall send an IAQ to LESC via Nlets in accordance with the Nlets Users Guide.

SYS2172 IAFIS (iDSM) shall accept an IAR from the LESC in accordance with the Nlets Operating Manual.

SYS2173 IAFIS (iDSM) shall accept an IAR from LESC that contains biographic information for a positive identification resulting from a Ten-Print Fingerprint Identification Search of the IDENT shared data records.

The biographic data will consist of DOB, Gender, the IDENT unique identifier (EID), the A-number, FNU, and Subject Name.

3.1.1.2.12 Ten-Print Processing Results

SYS60 ITN shall submit a positive identification response request to III for submissions containing fingerprints that match candidate fingerprints in the IAFIS repositories for file maintenance and response generation.

SYS61 ITN shall submit a non-identification response request to III for submissions containing fingerprints that do not match any candidate fingerprints in the IAFIS repositories for file maintenance and response generation.

SYS62 ITN shall notify AFIS when a non-identification or reject occurs for a Ten-Print Fingerprint Identification Search request for which the last feature fingerprint search produced candidates.

SYS63 IAFIS (ITN/TPS) shall provide the capability to print ten-print submissions that are non-identification to support manual Authorized FBI Service Provider searching of the Civil Files.

SYS64 ITN shall submit a criminal photo add request to III for submissions containing photos.

SYS2174 IAFIS (iDSM) shall forward an IAR from LESC to the Authorized Agency as a result of a positive identification on a Ten-Print Fingerprint Identification Search request of the IDENT shared data.

SYS65 IAFIS (III) shall process the file maintenance request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS66 ITN shall submit a fingerprint feature update request to AFIS for submissions containing fingerprints that match candidate fingerprints in the IAFIS repositories when image replacement is specified.

SYS67 ITN shall submit a fingerprint feature enrollment request to AFIS for submissions containing fingerprints that do not match any candidate fingerprints in the IAFIS repositories for file maintenance.

SYS68 IAFIS (ITN/ISRE) shall update a fingerprint image for submissions containing fingerprints that match candidate fingerprints in the IAFIS repositories when image replacement is specified.

SYS69 IAFIS (ITN/ISRE) shall add a fingerprint image for submissions containing fingerprints that do not match any candidate fingerprints in the IAFIS repositories for file maintenance.

SYS70 IAFIS (AFIS) shall perform a cascaded fingerprint search of the ULF, when appropriate, as part of the Ten-Print Fingerprint Identification Search request.

SYS71 IDWH shall extract User Fee Billing Data from ITN for completed Ten-Print Fingerprint Identification Search requests marked as user fee transactions.

SYS72 ITN shall submit the fingerprint processing decision to EFCON for routing to CSS.

IAFIS will indicate in the fingerprint processing decision, any actions necessary for CSS to perform, such as final routing or rescanning of the fingerprint cards.

SYS73 III shall send notifications to the appropriate internal and/or external parties upon completion of file maintenance as part of a Ten-Print Fingerprint Identification Search request.

SYS74 IAFIS (III) shall send a Hot Check Name Search request to NCIC upon completion of Ten-Print Fingerprint Identification subject criminal history file maintenance.

SYS75 IAFIS (ITN/TPS) shall forward non-identification humanitarian submission or other submissions indicating that a search of the manual file is required to Document Processing for a manual fingerprint file search.

Humanitarian submissions consist of unknown deceased, amnesia victims, or missing persons search requests.

3.1.1.3 Ten-Print Fingerprint Identification Outputs

SYS76 IAFIS (ITN/TPS) shall determine the response distribution method (i.e., electronic, hardcopy) for a Ten-Print Fingerprint Identification Search Response.

SYS77 IAFIS (EFCON) shall provide an Authorized Contributor with an identification decision as part of a Ten-Print Fingerprint Identification Search Response.

An identification decision will be either a positive identification or a non-identification. If the contributor is identified as not being capable of receiving electronic response, a hardcopy response will be generated and sent to the contributor, otherwise an electronic EFTS compliant response will be sent.

SYS2295 IAFIS (EFCON) shall return all fingerprint images to Authorized Contributors in 500ppi as part of a Ten-Print Fingerprint Identification Search response.

SYS78 IAFIS (III) shall provide the Subject Criminal History Rap Sheet for a candidate resulting in a positive identification as part of a Ten-Print Fingerprint Identification Search Response when requested.

SYS79 IAFIS (ITN) shall provide a reject response, as appropriate, for a Ten-Print Fingerprint Identification Search Request.

SYS80 IAFIS (ITN) shall provide a reason for rejection when the quality of the ten-print fingerprint characteristics is not sufficient to perform a fingerprint search or a repository maintenance action.

SYS81 IAFIS (EFCON) shall provide Authorized Contributors an electronic response to a Ten-Print Fingerprint Identification Search Request via the CJIS-WAN.

SYS82 IAFIS (ITN/TPS) shall provide the appropriate Ten-Print Fingerprint Identification Search response to an Authorized FBI Service Provider via the IAFIS Workstation.

SYS83 IAFIS (III) shall provide a hardcopy response to a Ten-Print Fingerprint Identification Search Request, as appropriate.

SYS84 IAFIS (III) shall provide an initial partial response when a Ten-Print Fingerprint Identification Search results in a positive identification to a manual record.

3.1.2 Latent Fingerprint Identification Services

The Latent Fingerprint Identification Services provides the capability to match fingerprint data from Latent Fingerprint Identification Search Requests to fingerprint data contained within the IAFIS fingerprint repositories. These searches result in an identification decision (i.e., positive identification, non-identification). If the submission does not meet minimum processing criteria (e.g., quality), the submission will be returned with a reason for rejection.

3.1.2.1 Latent Fingerprint Identification Inputs

SYS85 IAFIS (EFCON) shall accept fingerprint data from an Authorized Contributor as part of Latent Fingerprint Identification Search via the CJIS-WAN.

Latent Fingerprint Identification Search requests are only accepted from Authorized FBI Field Agencies.

SYS86 IAFIS (ITN/LPS) shall accept a Latent Fingerprint Identification Search Request via the IAFIS Workstation.

SYS87 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to scan fingerprint images to initiate a Latent Fingerprint Identification Search Request.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the

ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

SYS88 IAFIS (ITN/LPS) shall provide the capability for an authorized FBI Service Provider to submit a Latent Fingerprint Identification Search request to the Ten-Print Fingerprint Identification process.

SYS89 IAFIS (ITN/LPS) shall accept an indicator for enrollment into the Unsolved Latent File (ULF) as part of the Latent Fingerprint Identification Search Request.

SYS90 IAFIS (ITN/LPS) shall accept a fingerprint position indicator when a single fingerprint is submitted in a Latent Fingerprint Identification Search Request.

An FBI Service Provider can indicate which finger position to search against in the IAFIS repository. If the Latent Fingerprint Identification Search Request contains a single fingerprint image, the FBI Service Provider can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

SYS91 IAFIS (ITN/LPS) shall require finger position indicator(s) for each fingerprint when multiple fingerprints are submitted as part of a Latent Fingerprint Identification Search Request.

SYS92 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to specify the pattern classification for each fingerprint as part of a Latent Fingerprint Identification Search Request.

3.1.2.2 Latent Fingerprint Identification Processing

SYS93 ITN/TPS shall accept a Latent Fingerprint Identification Search request from ITN/LPS to be processed as a Ten-Print Fingerprint Identification Search request.

SYS94 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to manually extract fingerprint features from the fingerprint images provided in the Latent Fingerprint Identification Search Request.

SYS95 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to initiate automated fingerprint feature extraction to process a Latent Fingerprint Identification Search Request.

SYS96 IAFIS (ITN/LPS) shall require an authorized FBI Service Provider to extract (i.e., automated or manual) fingerprint features prior to processing a Latent Fingerprint Identification Search Request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

SYS97 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to manually enter data in support of Latent Fingerprint Identification processing.

SYS98 IAFIS (ITN/LPS) shall process Latent Fingerprint Identification submissions in the same manner as Ten-Print Fingerprint Identification submissions.

SYS99 IAFIS (ITN/LPS) shall require the authorized FBI Service Provider to perform a Manual FSC of the images provided in the Latent Fingerprint Identification Search prior to submitting the request to the Feature Search function. NGI-296

SYS100 IAFIS (ITN/LPS) shall provide the capability for an authorized FBI Service Provider to forward the fingerprint features extracted from the fingerprint images provided in the Latent Fingerprint Identification Search Request to the Feature Search function for searching of the specified IAFIS repository(s) using the finger position(s) provided.

Latent Fingerprint Identification Search Requests will be searched first against the criminal file. If no identification is made, the Latent Fingerprint Identification Search Request may then be searched against other IAFIS repositories (i.e., civil, Special Latent Cognizant, ULF).

SYS2296 IAFIS (ITN/LPS) shall require an Authorized FBI Service Provider to perform a manual special processing review when one or more candidates are marked with a special processing indicator (e.g., SPF) as part of a Latent Fingerprint Identification Search request.

SYS101 IAFIS (AFIS) shall provide the capability to reject the request when the quality of the latent fingerprint characteristics is not sufficient to perform a successful Latent Identification Search.

SYS102 IAFIS (AFIS) shall search with the fingerprint position indicated in the Latent Fingerprint Identification Search Request.

SYS103 IAFIS (AFIS) shall search all finger positions for a Latent Fingerprint Identification Search Request containing a single fingerprint when no finger position is indicated.

SYS104 IAFIS (AFIS) shall provide a ranked candidate list of a default number of FNUs as a result of a Latent Fingerprint Identification Search request.

SYS105 IAFIS (ITN/LPS) shall utilize the ITN/ISRE service when retrieving images in support of a Latent Fingerprint Identification Search request.

SYS106 IAFIS (ITN/LPS) shall retrieve composite images for each candidate as a result of a Latent Fingerprint Identification Search request.

SYS107 IAFIS (ITN/LPS) shall require an Authorized FBI Service Provider to perform a manual Latent Fingerprint Image Compare (LFIC) for each candidate for a Latent Fingerprint Identification Search Request.

SYS108 IAFIS (ITN/LPS) shall allow an Authorized FBI Service Provider to reject a Latent Fingerprint Identification Search Request as a result of the manual FIC.

SYS109 IAFIS (ITN/LPS) shall enroll subject information into the ULF, when appropriate, as a result of a Latent Fingerprint Identification Search Request.

3.1.2.3 Latent Fingerprint Identification Outputs

SYS110 IAFIS (ITN/LPS) shall compile response information for latent submissions and provide the compiled response information to III for final preparation, formatting and transmission.

SYS111 IAFIS (ITN/LPS) shall determine the response distribution method (i.e., electronic, hardcopy) for a Latent Fingerprint Identification Search Response.

SYS112 IAFIS (ITN/LPS) shall provide an Authorized Contributor with an identification decision as part of a Latent Fingerprint Identification Search Response via the CJIS-WAN.

NGI-297

An identification decision will be either a positive identification or non-identification.

SYS113 IAFIS (III) shall provide the Subject Criminal History Rap Sheet for a positively identified candidate in the Latent Fingerprint Identification Search Response when requested.

SYS114 IAFIS (ITN/LPS) shall provide a reject response, as appropriate, for a Latent Fingerprint Identification Search Request.

SYS115 IAFIS (ITN/LPS) shall provide a reason for rejection when the quality of the latent fingerprint characteristics is not sufficient to perform a Latent Fingerprint Identification Search request.

SYS116 IAFIS (EFCON) shall provide a response to a Latent Fingerprint Identification Search request from an Authorized Contributor via the CJIS-WAN.

SYS117 IAFIS (III) shall provide a hardcopy response to a Latent Fingerprint Identification Search Request, as appropriate.

SYS118 IAFIS (ITN/TPS) shall provide the appropriate Latent Fingerprint Identification Search response to an Authorized FBI Service Provider via the IAFIS Workstation.

3.2 Verification Services Functional Requirements

There are no system requirements to support IAFIS Verification User Services.

3.3 Information Services System Requirements

The following section contains the system level requirements that support the IAFIS Information User Services.

3.3.1 Fingerprint Image Retrieval Request

The Fingerprint Image Retrieval Request provides the capability to retrieve fingerprint images or latent images using the ISRE function for records contained within the IAFIS repositories. The requester provides the FBI Number(s), CRN, SCNA or other identifiers for the subject(s) whose images are being requested. As a result of this request, IAFIS will provide image data for the specified subject.

3.3.1.1 Fingerprint Image Retrieval Request Inputs

SYS119 IAFIS (EFCON) shall accept Fingerprint Image Retrieval Requests via the CJIS WAN.

SYS120 IAFIS (ITN/TPS) shall accept Fingerprint Image Retrieval Requests via the IAFIS Workstation.

SYS121 IAFIS (EFCON) shall accept up to 1000 subjects' records as part of a single Fingerprint Image Retrieval Request.

3.3.1.2 Fingerprint Image Retrieval Request Processing

SYS122 IAFIS (III) shall process the Fingerprint Image Retrieval request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS123 IAFIS (ITN/ISRE) shall retrieve the composite fingerprint image for each specified subject (e.g., FBI Number, CRN, SCNA) as part of the Fingerprint Image Retrieval Request.

IAFIS will generate ISRE record requests to retrieve records from the ISRE image file.

SYS124 IAFIS (ITN/ISRE) shall reject a Fingerprint Image Retrieval Request when the specified subject image does not exist.

3.3.1.3 Fingerprint Image Retrieval Request Outputs

SYS125 IAFIS (EFCON) shall provide an electronic Fingerprint Image Retrieval Response via the CJIS WAN.

SYS126 IAFIS (ITN/TPS) shall allow an authorized FBI Service Provider to view the images returned from the Fingerprint Image Retrieval Request on an IAFIS Workstation.

SYS127 IAFIS (ITN/ISRE) shall provide the fingerprint images retrieved as part of a Fingerprint Image Retrieval Response.

SYS128 IAFIS (ITN/TPS) shall provide individual Fingerprint Image Request Responses for each subject record identifier number provided in the request.

SYS129 IAFIS (III) shall provide a summary report listing each subject's images that were returned from the Fingerprint Image Retrieval Request.

SYS130 IAFIS (ITN/TPS) shall provide a reject message to a Fingerprint Image Retrieval Request when appropriate.

SYS131 IAFIS (ITN/TPS) shall include a reason(s) for the rejection in the Fingerprint Image Request Response, if IAFIS was unsuccessful in retrieving the specified fingerprint images designated in the request.

3.3.2 Criminal Photo Image Retrieval Request

The Criminal Photo Image Retrieval request enables users to retrieve a criminal photo set from the IAFIS Repository. Each photo set for a criminal record (identified by an FBI number) is linked to the subject by the Date of Arrest (DOA).

3.3.2.1 Criminal Photo Image Retrieval Request Inputs

SYS132 IAFIS (EFCON) shall accept Criminal Photo Image Retrieval Requests via the CJIS WAN.

3.3.2.2 Criminal Photo Image Retrieval Request Processing

SYS133 IAFIS (III) shall process the Criminal Photo Image Retrieval request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

NGI-299

SYS134 IAFIS (III/IPS) shall retrieve the most recently taken set of photos for the FBI number

designated in the Criminal Photo Image Retrieval Request, when no specific criminal event information (e.g., DOA) is specified.

SYS135 IAFIS (III/IPS) shall retrieve the photo set for the specified criminal event designated in the Criminal Photo Image Retrieval Request.

SYS136 IAFIS (III/IPS) shall reject a Criminal Photo Image Retrieval Request when the specified subject identifier does not exist.

SYS137 IAFIS (III/IPS) shall reject a Criminal Photo Image Retrieval Request when the specified criminal event identifier does not exist.

3.3.2.3 Criminal Photo Image Retrieval Request Outputs

SYS138 IAFIS (EFCON) shall provide an electronic Criminal Photo Image Retrieval Response via the CJIS WAN.

SYS139 IAFIS (III/IPS) shall provide the photo set retrieved as part of the Criminal Photo Image Retrieval Response

SYS140 IAFIS (III/IPS) shall include a reason(s) for the rejection in the Criminal Photo Image Retrieval Response, if IAFIS was unsuccessful in retrieving the specified photo set designated in the request.

3.3.3 Criminal History Request

3.3.3.1 Criminal History Request Inputs

SYS141 IAFIS (III) shall accept Criminal History Requests via NCIC.

SYS2162 IAFIS (III) shall accept bulk Criminal History Requests via EFCON electronic message.

SYS142 IAFIS (ITN/TPS) shall accept Criminal History Requests via the IAFIS Workstation.

SYS143 IAFIS (ITN/TPS) shall accept Civil Subject Index Master File Requests via the IAFIS Workstation.

SYS144 IAFIS (ITN/TPS) shall provide the capability for the authorized FBI Service Provider to request a Receiving Agency Notification Report as part of the Criminal History Request via the IAFIS Workstation.

SYS145 IAFIS (ITN/TPS) shall provide the capability for the authorized FBI Service Provider to request a Record Set Report as part of the Criminal History Request via the IAFIS Workstation.

3.3.3.2 Criminal History Request Processing

SYS146 IAFIS (III) shall retrieve the Criminal History information for the specified subject as part of the Criminal History Request.

SYS147 IAFIS (III) shall retrieve the Civil Subject Index Master File Information for the specified subject as part of the Civil Subject Index Master File Request.

SYS148 IAFIS (III) shall reject a Criminal History Request when the specified subject identifier does not exist.

SYS149 IAFIS (III) shall reject a Civil Subject Index Master File Request when the specified subject identifier does not exist.

3.3.3.3 Criminal History Request Outputs

SYS150 IAFIS (III) shall determine the response distribution method (i.e., electronic, hardcopy) for a Criminal History Request response.

SYS2163 IAFIS (EFCON) shall determine the response distribution method (i.e., electronic, hardcopy media) for a bulk Criminal History Request response.

SYS151 IAFIS (III) shall provide a Criminal History Response via NCIC.

SYS152 IAFIS (III) shall provide to the requestor a list of the state(s) that maintain the criminal history data for the subject of interest, for NCIC Criminal History responses where ownership responsibility of the criminal history data resides with a III participating state or an NFF state.

SYS153 IAFIS (III) shall request the owner state(s) to forward the data depending on the requester's capabilities, for NCIC Criminal History responses where ownership responsibility of the criminal history data resides with a III participating state or an NFF state.

SYS154 IAFIS (III) shall send messages to III/NFF participating states requesting that they send their arrest information to the requestor, for NCIC Criminal History responses.

Criminal History Responses will include responses of Type 1, Type 2, and Type 3.

SYS155 IAFIS (III) shall provide the Subject Criminal History Rap Sheet for the specified subject in a Criminal History Request response.

SYS156 IAFIS (III) shall provide the Receiving Agency Notification Report when requested for the specified subject in a Criminal History Request response.

SYS157 IAFIS (III) shall provide the Record Set Report when requested for the specified subject in a Criminal History Request response.

SYS158 IAFIS (III) shall provide a hardcopy response to a Criminal History Request, as appropriate.

SYS159 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Provider to view the Criminal History Request response on an IAFIS Workstation.

SYS160 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Provider to print the Criminal History Request response.

SYS161 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Provider to view the Civil Subject Index Master File Request response on an IAFIS Workstation.

Civil Subject Index Master File Responses will include only Type 1 Responses with no arrest history pointers.

SYS162 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Provider to print the Civil Subject Index Master File response.

SYS163 IAFIS (ITN/TPS) shall provide a reject response to a Criminal History Request when appropriate.

SYS164 IAFIS (ITN/TPS) shall include a reason(s) for the rejection in the Criminal History Response, if IAFIS was unsuccessful in retrieving the specified Criminal History designated in the request.

3.3.4 Certification File Request

3.3.4.1 Certification File Request Inputs

SYS165 IAFIS (ITN/TPS) shall accept a Certification File Request via an IAFIS Workstation.

SYS166 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Provider to indicate the specific Ten-Print Certification File (TPCF) index to be retrieved from the TPCF.

3.3.4.2 Certification File Request Processing

SYS167 IAFIS (ITN/TPS) shall retrieve the Certification File Record, using the TPCF index, for the specified subject and unique event as part of the Certification File Request.

SYS168 IAFIS (ITN/TPS) shall reject the Certification File Request when the Subject Identifier or transaction identifier is invalid.

3.3.4.3 Certification File Request Outputs

SYS169 IAFIS (ITN/TPS) shall allow an authorized FBI Service Provider to view the Certification File Request response on an IAFIS Workstation.

SYS170 IAFIS (ITN/TPS) shall provide the capability for a Authorized FBI Service Provider to print the retrieved Certification File Record without having it displayed on the IAFIS workstation.

IAFIS will ensure that the printout conforms to the ten-print card standard to which it applies, as described in the *Specification for CJIS Division Fingerprint Cards*, ten-print card standards for FD-249 Criminal, FD-258 Applicant, and FD-353 Personal Identification fingerprint cards.

3.3.5 Other Information Requests

Other information requests processed by IAFIS include the Record Availability Inquiry and the Administrative Inquiry. The Record Availability Inquiry (ZR) is used to determine, by providing a FBI or SID number, if a subject record is on file in the III. The Administrative Inquiry (ZI) is used by III participants when there is a need to determine: the presence of a SID or FBI pointer and the date established; single-, multi-state or wanted status; or dates of establishment and/or last update.

3.3.5.1 Other Information Requests Input

SYS171 IAFIS (III) shall accept Record Availability Inquiries via NCIC.

SYS172 IAFIS (III) shall accept Administrative Inquiries via NCIC.

SYS173 IAFIS (III) shall accept Record Status Inquiries via NCIC.

3.3.5.2 Other Information Requests Processing

SYS174 IAFIS (III) shall process a Record Availability Inquiry to determine if a subject exists in the Subject Criminal History File with the requesting FBI or SID number.

SYS175 IAFIS (III) shall process an Administrative Inquiry to determine if the Subject Criminal History File subject provided is a single-state or multi-state.

SYS176 IAFIS (III) shall process an Administrative Inquiry to determine the date that the record was established.

SYS177 IAFIS (III) shall process an Administrative Inquiry to determine the date that the record was last updated.

SYS178 IAFIS (III) shall process a Record Status Inquiry to determine the subject status in the Subject Criminal History File with the requesting FBI or SID number.

3.3.5.3 Other Information Requests Outputs

SYS179 IAFIS (III) shall provide a response to a Record Availability Inquiry via NCIC.

SYS180 IAFIS (III) shall provide a response to an Administrative Inquiry via NCIC.

SYS181 IAFIS (III) shall provide a response to a Record Status Inquiry via NCIC.

3.4 Investigation Services Functional Requirements

The following section contains the functional requirements supporting IAFIS Investigation User Services.

3.4.1 Subject Search Request

IAFIS provides a subject search capability that matches physical and biographic descriptors with physical and biographic descriptors contained in the Subject Criminal History or Civil Files.

3.4.1.1 Subject Search Request Inputs

SYS182 IAFIS (III) shall accept Subject Search Requests via NCIC.

SYS183 IAFIS (III) shall accept a Subject Search Request via Machine Readable Data (MRD).

SYS184 IAFIS (ITN) shall allow an Authorized FBI Service Provider to submit a Subject Search Request via an IAFIS Workstation.

The Service Provider Subject Search (SPSS) Request received via the IAFIS Workstation can be initiated by an IAFIS TPS, DPS, or LPS Service Provider, or by a NICS Examiner. The Federal Agency Subject Search (FASS) Request received via the IAFIS Workstation can be initiated by only the DPS Service Providers.

SYS185 III shall accept a Subject Search Request from ITN/TPS as part of a Ten-Print Fingerprint Identification Search request. NGI-303

SYS186 IAFIS (ITN) shall allow an Authorized FBI Service Provider to designate a repository to search as part of a Subject Search Request.

SYS187 IAFIS (III) shall accept Subject Identifiers (i.e., FNU, CRN, SID), subject name, DOB, sex and race as biographic descriptor data for a Subject Search Request.

Optional descriptor data may include: aliases (AKAs), social security number, miscellaneous numbers (such as military service number or operator's license number), State Identification Number (SID), FBI Number, race, height, weight, eye color, hair color, Scars, Marks, and Tattoos (SMT) and place of birth.

FBI numbers and SIDs are unique. Therefore, if either number is used as a descriptor, the search of the file is bypassed and the single candidate record is retrieved from the file. If no record in the file matches, a "no record" message is provided.

3.4.1.2 Subject Search Request Processing

SYS188 IAFIS (III) shall search the repository designated as part of the Subject Search Request.

SYS189 IAFIS (III) shall search the Subject Criminal History repository by default when no repository is designated in the Subject Search Request.

SYS190 IAFIS (III) shall perform a search using the biographic data contained in the Subject Search Request.

SYS191 IAFIS (III) shall perform a subject search based on name, date of birth, gender, and race when provided in an NCIC Subject Search request.

SYS192 IAFIS (III) shall retrieve candidate(s) based on social security number when provided in a subject search request.

SYS193 IAFIS (III) shall retrieve candidate(s) based on miscellaneous number when provided in a subject search request.

SYS194 IAFIS (III) shall retrieve candidate(s) based on State Identification Number (SID) when provided in a subject search request.

SYS195 IAFIS (III) shall retrieve candidate(s) based on an FBI Number when provided in a subject search request.

SYS196 IAFIS (III) shall bypass the subject search process and retrieve the single candidate when an FBI Number or SID is included and the number references a subject in the Subject Criminal History File.

SYS197 IAFIS (III) shall combine the candidates returned from the subject search with the candidates directly retrieved into a single ranked candidate list as part of a subject search request.

SYS198 IAFIS (III) shall provide a ranked candidate list with zero or more candidates in response to a subject Search request.

SYS199 IAFIS (III) shall return up to the maximum number of candidates in response to a Subject Search request.

SYS200 IAFIS (III) shall include, on the subject search candidate list, the candidates with match scores above the applicable threshold.

SYS201 IAFIS (III) shall process the Subject Search request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS202 IAFIS (III) shall reject a subject search request when the subject is unsuccessful.

3.4.1.3 Subject Search Request Outputs

SYS203 IAFIS (III) shall determine the response distribution method (i.e., electronic, hardcopy) for a Subject Search Request response.

SYS204 IAFIS (III) shall provide an electronic Subject Search Request via NCIC.

SYS205 IAFIS (III) shall write to removable media a candidate list in response to an MRD Subject Search Request.

SYS206 IAFIS (III) shall provide a hardcopy of a candidate's criminal history Rap Sheet for each candidate in response to an MRD Subject Search Request.

SYS207 III shall provide the appropriate Subject Search response to ITN/TPS as part of the Ten-Print Fingerprint Identification Search request.

SYS208 IAFIS (ITN) shall provide the appropriate Subject Search response to an authorized FBI Service Provider via the IAFIS Workstation.

SYS209 IAFIS (ITN) shall allow an authorized FBI Service Provider to view the candidate list returned from the Subject Search Request using an IAFIS Workstation.

SYS210 IAFIS (ITN) shall allow an authorized FBI Service Provider to view the subject history returned as the single candidate from the Subject Search Request using an IAFIS Workstation.

SYS211 IAFIS (ITN) shall allow an authorized FBI Service Provider to print the candidate list returned from the Subject Search Request using an IAFIS Workstation.

SYS212 IAFIS (ITN) shall allow an authorized FBI Service Provider to print the subject history returned as the single candidate from the Subject Search Request using an IAFIS Workstation.

SYS213 IAFIS shall include the reason(s) for rejection of the Subject Search Request.

3.4.2 Ad Hoc Subject Search

3.4.2.1 Ad Hoc Subject Search Inputs

SYS214 IAFIS (ITN) shall accept an Ad Hoc Subject Search Request via an IAFIS Workstation.

The Ad Hoc Subject Search Request received via the IAFIS Workstation can be initiated by an IAFIS TPS, DPS, or LPS Service Provider.

SYS215 IAFIS (ITN) shall allow an Authorized FBI Service Provider to designate an IAFIS repository to search as part of the Ad Hoc Subject Search request.

The FBI Service Provider may direct the Ad Hoc Subject Search against either the Subject Criminal History File or the Civil Subject Index Master File.

SYS216 IAFIS (ITN) shall accept Subject Identifiers (i.e., FNU, CRN, SID), subject name,

DOB, sex, race as biographic descriptor data for an Ad Hoc Subject Search request.

SYS217 IAFIS (ITN) shall accept criminal history data as part of an Ad Hoc Subject Search Request.

SYS218 IAFIS (ITN) shall accept multiple entries of all Ad Hoc Subject Search parameters.

SYS219 IAFIS (ITN) shall allow the authorized FBI Service Provider to specify which parameters should be combined using the Boolean set operators union and intersection to determine the matching candidates as part of an Ad Hoc Subject Search request.

SYS220 IAFIS (ITN) shall allow the authorized FBI Service Provider to submit an Ad Hoc Subject Search using a free-text command line as part of the Ad Hoc Subject Search request.

SYS221 IAFIS (ITN) shall allow the authorized FBI Service Provider to specify that a candidate list be generated in response to an Ad Hoc Subject Search request.

SYS222 IAFIS (ITN) shall allow the authorized FBI Service Provider to specify the maximum number of candidates to be returned as part of an Ad Hoc Subject Search response.

3.4.2.2 Ad Hoc Subject Search Processing

SYS223 IAFIS (III) shall search the repository designated as part of the Ad Hoc Subject Search request.

SYS224 IAFIS (III) shall search the Subject Criminal History repository by default when no repository is designated in the Ad Hoc Subject Search request.

SYS225 IAFIS (III) shall perform a search using the biographic data contained in the Ad Hoc Subject Search request.

SYS226 IAFIS (III) shall perform a search using the criminal history data contained in the Ad Hoc Subject Search request.

SYS227 IAFIS (ITN) shall allow an Authorized FBI Service Provider to enter the desired values of the elements specified in the Civil Ad Hoc Search Parameter Table 3.4.2-1, as part of an Ad Hoc Subject Search of the Civil Subject Index Master File.

SYS228 IAFIS (ITN) shall allow an Authorized FBI Service Provider to modify the Ad Hoc Subject Search Parameters specified in the Civil Ad Hoc Search Parameter Table 3.4.2-1.

SYS229 IAFIS (ITN) shall allow an Authorized FBI Service Provide to enter the desired values of the elements specified in the Criminal Ad Hoc Search Parameter Table 3.4.2-2, as part of an Ad Hoc Subject Search of the Criminal Index Master File.

SYS230 IAFIS (ITN) shall allow an Authorized FBI Service Provider to modify the Ad Hoc Subject Search Parameters specified in the Criminal Ad Hoc Search Parameter Table 3.4.2-2.

SYS231 IAFIS (III) shall identify all subjects in the designated IAFIS repository that match the search criteria provided in the ad hoc subject search inquiry.

Table 3.4.2-1 Civil Ad Hoc Search Parameter Table

Element	Search Parameter Modifiers*		
	Ranges	Not	Wildcards
CIVIL BIOGRAPHICAL DESCRIPTOR DATA			

Element	Search Parameter Modifiers*		
	Ranges	Not	Wildcards
Name	—	—	Yes
Alias	—	—	Yes
Date of birth	Yes	—	—
Place of birth		Yes	
CIVIL PHYSICAL DESCRIPTOR DATA			
Gender	—	Yes	—
Race	—	Yes	—
Height	Yes	—	—
Weight	Yes	—	—
Eye color	—	Yes	—
Hair color	—	Yes	—
Scars, marks, and tattoos	—	—	—
OTHER SEARCH PARAMETERS			
Social Security Number	—	—	—
Miscellaneous ID numbers (licenses, etc.)	—	—	—

* Search parameter modifiers operate on the parameters in the following ways:

Range: Includes all values of the parameter between the lower and upper bounds provided in the request

Not: Includes all allowable values of the parameter except what is explicitly provided in the request

Wildcard: Includes all values of the parameter that match at least the explicitly provided characters

Table 3.4.2-2 Criminal Ad Hoc Search Parameter Table

Element	Search Parameter Modifiers*		
	Ranges	Not	Wildcards
CRIMINAL BIOGRAPHICAL DESCRIPTOR DATA			
Name	---	---	Yes
Alias	---	---	Yes
Date of birth	Yes	---	---
Place of birth	---	Yes	---
Identification comments	---	---	Yes
CRIMINAL PHYSICAL DESCRIPTOR DATA			
Gender	---	Yes	---
Race	---	Yes	---
Height	Yes	---	---
Weight	Yes	---	---
Eye color	---	Yes	---
Hair color	---	Yes	---
Scars, marks, and tattoos	---	---	---
ARREST DATA			
Date of arrest	Yes	---	---
Additional arrest disposition data	---	---	Yes

NGI 307

Element	Search Parameter Modifiers*		
	Ranges	Not	Wildcards
Referenced Originating Agency Identification Number	---	---	---
Referenced date	Yes	---	---
Arrest offense literal	---	---	Yes
Statute citation	---	---	---
Originating agency identifier (ORI)	---	---	---
Date of offense	---	---	---
Type of offense	---	---	---
OTHER SEARCH PARAMETERS			
Social Security Number	---	---	---
Miscellaneous ID numbers (licenses, etc.)	---	---	---
Fingerprint Classification (NCIC and Pattern) and finger number	----	---	---

* Search parameter modifiers operate on the parameters in the following ways:

Range: Includes all values of the parameter between the lower and upper bounds provided in the request

Not: Includes all allowable values of the parameter except what is explicitly provided in the request

Wildcard: Includes all values of the parameter that match at least the explicitly provided characters

3.4.2.3 Ad Hoc Subject Search Outputs

SYS232 IAFIS (III) shall provide the Ad Hoc Subject Search response data via the IAFIS Workstation.

SYS233 IAFIS (III) shall provide a reject response, when appropriate, as a result of an Ad Hoc Subject Search request.

SYS234 IAFIS (III) shall provide a ranked candidate list of FNUs or CRNs up to the maximum number of candidates as part of the response to the Ad Hoc Subject Search Request.

SYS235 IAFIS (III) shall return the number of candidates specified by the Authorized FBI Service Provider as part of the Ad Hoc Subject Search request.

SYS236 IAFIS (III) shall return the default number of candidates when number of candidates is not specified as part of an Ad Hoc Subject Search.

SYS237 IAFIS (ITN) shall display the candidate list and a numeric indicator of the number of candidates found that fulfill the search criteria as part of the Ad Hoc Subject Search Request.

SYS238 IAFIS (ITN) shall allow an Authorized FBI Service Provider to view the candidate list returned from the Ad Hoc Subject Search Request.

SYS239 IAFIS (ITN) shall allow an Authorized FBI Service Provider to print the candidate list returned from the Ad Hoc Subject Search Request.

SYS240 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to copy the Ad Hoc Subject Search resulting candidate(s) to an SLC File.

Only a limited number of Authorized Service Providers will be provided the capability to copy Ad Hoc Subject Search candidate(s) to a SLC.

3.4.3 Ten-Print Fingerprint Image Search

An Authorized Contributor will be able to submit a Ten-Print Fingerprint Image Search request with fingerprint images, fingerprint classification information, and biographic descriptors. The response consists of a candidate list and the fingerprint images of the highest ranked candidate.

3.4.3.1 Ten-Print Fingerprint Image Search Inputs

SYS241 IAFIS (EFCON) shall accept Ten-Print Fingerprint Image Search requests from an Authorized Contributor via the CJIS WAN.

3.4.3.2 Ten-Print Fingerprint Image Search Processing

SYS242 IAFIS (AFIS) shall perform an automated image quality check on a Ten-Print Fingerprint Image Search request based on image quality standards.

SYS243 IAFIS (AFIS) shall automatically extract fingerprint features from the fingerprint images provided in the Ten-Print Fingerprint Image Search request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

SYS244 IAFIS (AFIS) shall search the IAFIS criminal fingerprint repository using the fingerprint classification data, biographic data, and extracted fingerprint features from the Ten-Print Fingerprint Image Search requests.

SYS245 IAFIS (III) shall process the Ten-Print Fingerprint Image Search request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS246 IAFIS (ITN/TPS) shall retrieve the composite fingerprint images using the ISRE function for the highest ranking candidate as a result of Ten-Print Fingerprint Image Search request.

Images for the remaining candidates may be retrieved through separate Fingerprint Image Retrieval requests using the remaining FNUs provided in the Ten-Print Fingerprint Image Search response.

SYS247 IAFIS (AFIS) shall reject a Ten-Print Fingerprint Image Search request when the fingerprint images fail to satisfy minimum image quality standards.

3.4.3.3 Ten-Print Fingerprint Image Search Outputs

SYS248 IAFIS (EFCON) shall provide an electronic response to a Ten-Print Fingerprint Image Search request via the CJIS WAN.

SYS249 IAFIS (AFIS) shall provide a ranked candidate list of FNUs for up to the maximum number of candidates as a result of the Ten-Print Fingerprint Image Search request.

The response to a Ten-Print Fingerprint Image Search includes a candidate list comprised of the names and FBI numbers of up to 25 subjects as potential matches to the fingerprint images that were submitted. The fingerprint image(s) of the first candidate on the candidate list will also be included. The fingerprint images in the response may be specified by finger position in the search request.

NGI-309

SYS250 IAFIS (ITN/TPS) shall provide a reject message to a Ten-Print Fingerprint Image Search request when appropriate.

SYS251 IAFIS (ITN/TPS) shall include a reason(s) for the rejection in the Ten-Print Fingerprint Image Search response.

3.4.4 Ten-Print Fingerprint Feature Search

The Ten-Print Fingerprint Feature Search requests will allow an Authorized Contributor to search using fingerprint features, pattern classification, and biographic descriptors. The response consists of a candidate list and the fingerprint images of the highest ranked candidate.

3.4.4.1 Ten-Print Fingerprint Feature Search Inputs

SYS252 IAFIS (EFCON) shall accept Ten-Print Fingerprint Feature Search requests from an Authorized Contributor via the CJIS WAN.

3.4.4.2 Ten-Print Fingerprint Feature Search Processing

SYS253 IAFIS (AFIS) shall search the IAFIS criminal fingerprint repository using the fingerprint features, fingerprint classification, and biographic data contained within the Ten-Print Fingerprint Feature Search request.

SYS254 IAFIS (III) shall process the Ten-Print Fingerprint Feature Search request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS255 IAFIS (ITN/TPS) shall retrieve the composite fingerprint images using the ISRE function for the highest ranking candidate as a result of Ten-Print Fingerprint Feature Search request.

Images for the remaining candidates may be retrieved through separate Fingerprint Image Retrieval requests using the remaining FNUs provided as part of the Ten-Print Fingerprint Feature Search response.

3.4.4.3 Ten-Print Fingerprint Feature Search Outputs

SYS256 IAFIS (EFCON) shall provide an electronic response to a Ten-Print Fingerprint Feature Search request via the CJIS WAN.

SYS257 IAFIS (AFIS) shall provide a ranked candidate list of FNUs for up to the maximum number of candidates as a result of the Ten-Print Fingerprint Feature Search request.

The response to a Ten-Print Fingerprint Feature Search includes a candidate list comprised of the names and FBI numbers of up to 25 subjects as potential matches to the fingerprint features that were submitted. The fingerprint image(s) of the first candidate on the candidate list will also be included. The fingerprint images in the response may be specified by finger position in the search request.

3.4.5 Ten-Print Fingerprint Rap Sheet Search

An Authorized Contributor will submit a Ten-Print Fingerprint Rap Sheet Search request with fingerprint images, fingerprint classification information, and biographic descriptors. The response to

this search will consist of a candidate list containing up to 20 candidates and the corresponding rap sheets.

3.4.5.1 Ten-Print Fingerprint Rap Sheet Search Inputs

SYS258 IAFIS (EFCON) shall accept Ten-Print Fingerprint Rap Sheet Search request from an Authorized Contributor via the CJIS WAN.

3.4.5.2 Ten-Print Fingerprint Rap Sheet Search Processing

SYS259 IAFIS (AFIS) shall perform an automated image quality check on a Ten-Print Fingerprint Rap Sheet Search request based on image quality standards.

SYS260 IAFIS (AFIS) shall automatically extract fingerprint features from the fingerprint images provided in the Ten-Print Fingerprint Rap Sheet Search Request.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

SYS261 IAFIS (AFIS) shall search the criminal fingerprint repository using the fingerprint classification data and extracted fingerprint features from the Ten-Print Fingerprint Rap Sheet Search Request.

SYS262 IAFIS (III) shall process the Ten-Print Fingerprint Rap Sheet Search request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS263 IAFIS (III) shall retrieve the subject criminal history identifier and rap sheet for the highest ranked candidate(s) up to the maximum number as a result of Ten-Print Fingerprint Rap Sheet Search Request.

SYS264 IAFIS (AFIS) shall reject a Ten-Print Fingerprint Rap Sheet Search request when the fingerprint images fail to satisfy minimum image quality standards.

3.4.5.3 Ten-Print Fingerprint Rap Sheet Search Outputs

SYS265 IAFIS (EFCON) shall provide an electronic response to a Ten-Print Fingerprint Rap Sheet Search request via the CJIS WAN.

The search response may contain up to 20 top-scoring candidates in addition to any subject criminal history records associated with those candidates.

SYS266 IAFIS (III) shall provide the Subject Criminal History Rap Sheet for all candidates in the Ten-Print Fingerprint Rap Sheet Search Response.

Images will not be provided as part of the Ten-Print Fingerprint Rap Sheet Search response.

3.4.6 Latent Penetration Query

The Latent Penetration Query allows the user to request an estimated percentage of the IAFIS repository that will be accessed by a Latent Fingerprint Image Search request or a Latent Fingerprint Feature Search request. The query contains the search parameters that will be defined in the search but no images or features. This transaction applies only to a single finger even if the original transaction

included multiple fingers.

3.4.6.1 Latent Penetration Query Inputs

SYS267 IAFIS (EFCON) shall accept Latent Penetration Query requests from Authorized Contributors via the CJIS WAN.

SYS268 IAFIS (ITN/LPS) shall accept Latent Penetration Query requests from an Authorized FBI Service Provider via an IAFIS Workstation.

3.4.6.2 Latent Penetration Query Processing

SYS269 IAFIS (AFIS) shall calculate the estimated percentage of the IAFIS repository that would be searched using the provided set of search-limiting parameters as part of a Latent Penetration Query.

SYS270 IAFIS (AFIS) shall maintain a statistical representation of the composition of the Criminal Repository, sufficient to estimate repository penetration.

SYS271 IAFIS (AFIS) shall provide the capability to report unsuccessful search parameters and the calculated percentage of the search population for a latent search transaction where the dynamically determined percentage of the repository population to be searched is greater than the designated cap.

3.4.6.3 Latent Penetration Query Outputs

SYS272 IAFIS (EFCON) shall provide an electronic response to a Latent Penetration Query request via the CJIS WAN.

SYS273 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to view the results of the Latent Penetration Query request on an IAFIS Workstation.

3.4.7 Latent Fingerprint Image Search

The Latent Fingerprint Image Search request will contain fingerprint image(s), fingerprint classification information, and biographic descriptors. The fingerprint features will be automatically extracted from the images with no human intervention. Latent Fingerprint Image and Latent Fingerprint Feature Search requests are processed exactly the same except for the fact that IAFIS performs an automated feature extraction as part of Latent Fingerprint Image Search requests. In the event that images are of insufficient quality to successfully extract the features and perform a search, IAFIS will respond with a Latent Transaction Error message.

There will be no manual editing of fingerprint characteristics for Latent Fingerprint Image Searches. IAFIS will conduct the search and will transmit the results to the originator. The response to a Latent Fingerprint Image Search consists of a candidate list of FNUs and fingerprint images.

3.4.7.1 Latent Fingerprint Image Search Inputs

SYS274 IAFIS (EFCON) shall accept Latent Fingerprint Image Search requests from an Authorized Contributor via CJIS WAN.

NGI-312

3.4.7.2 Latent Fingerprint Image Search Processing

SYS275 IAFIS (AFIS) shall process Latent Fingerprint Image Search requests in priority order.

SYS276 IAFIS (AFIS) shall support multiple priority levels for Latent Fingerprint Image Search requests from state and local users.

Priorities will generally correspond to the following crime types:

- Homicide, rape, and special circumstances
- Kidnap, assault, and robbery
- Arson, drugs, personal crimes, and property crimes

Federal agencies will determine their own priority schemes. No additional validation of priorities will be provided. IAFIS will not interrupt searches in progress upon receipt of higher priority searches.

SYS277 IAFIS (AFIS) shall determine the percentage of file penetration based on the information provided in the Latent Fingerprint Image Search request.

SYS278 IAFIS (AFIS) shall reject the Latent Fingerprint Image Search when the percentage of file penetration exceeds the maximum allowable file penetration for the target repository.

SYS279 IAFIS (AFIS) shall provide the capability to treat multiple finger searches as a single Latent Fingerprint Image Search request with a single file penetration percentage.

SYS280 IAFIS (AFIS) shall extract image features from the image(s) provided in the Latent Fingerprint Image Search request.

The features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

SYS281 IAFIS (AFIS) shall perform an image quality check on a Latent Fingerprint Image Search request based on quality standards.

SYS282 IAFIS (AFIS) shall reject a Latent Fingerprint Image Search request when the images fail to satisfy minimum quality standards.

SYS283 IAFIS (AFIS) shall provide the capability to search using one or more fingers as part of a Latent Fingerprint Image Search request.

SYS284 IAFIS (AFIS) shall utilize the Feature Search functionality when processing a Latent Fingerprint Image Search request using the features extracted from the image.

SYS285 IAFIS (AFIS) shall search the criminal fingerprint repository as part of a Latent Fingerprint Image Search request.

SYS286 IAFIS (AFIS) shall search using the finger position(s), fingerprint classification data, biographic data, and extracted features provided as part of a Latent Fingerprint Image Search request.

SYS287 IAFIS (AFIS) shall search all finger positions when a single image is provided and no fingerprint position is indicated on the Latent Fingerprint Image Search request.

SYS288 IAFIS (AFIS) shall search the image against all the finger positions provided when a

single image is provided along with multiple finger positions in the Latent Fingerprint Image Search request.

SYS289 IAFIS (AFIS) shall reject the Latent Fingerprint Image Search request with multiple images are provided and no unique finger position is included with each image.

SYS290 IAFIS (III) shall process the Latent Fingerprint Image Search candidate list according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS291 IAFIS (ITN/TPS) shall provide a ranked candidate list including names, FNUs, match scores, and matching finger positions as a result of the Latent Fingerprint Image Search request.

IAFIS will return 20 candidate FNUs as the result of a Latent Fingerprint Image Search request.

SYS292 IAFIS (ITN/TPS) shall utilize the ISRE retrieval functionality when retrieving images in support of a Latent Fingerprint Image Search request.

SYS293 IAFIS (ITN/ISRE) shall retrieve the indicated number of images, with a default of one, and the associated information as part of a Latent Fingerprint Image Search request.

SYS294 IAFIS (ITN/ISRE) shall retrieve the matching fingerprint image from the candidate ten-print records as part of a Latent Fingerprint Image Search request.

SYS295 IAFIS (AFIS) shall enroll subject feature information into the ULF, when indicated, as a result of a Latent Fingerprint Image Search request.

SYS296 IAFIS (ITN/ISRE) shall enroll subject image information into the ULF, when indicated, as a result of a Latent Fingerprint Image Search request.

SYS297 IAFIS (AFIS) shall temporarily add the fingerprint characteristics and descriptive data to the ULF when the Latent Fingerprint Image Search request includes the ULF add indication.

IAFIS (AFIS) will use all temporary records in subsequent searches of the ULF.

SYS298 IAFIS (AFIS) shall provide the capability to designate the appropriate ULF record as permanent when an "add confirm" message is received as part of a Latent Fingerprint Image Search request.

3.4.7.3 Latent Fingerprint Search Outputs

SYS299 IAFIS (EFCON) shall provide the appropriate Latent Fingerprint Image Search response to the Authorized Contributor via the CJIS WAN.

SYS300 IAFIS (AFIS) shall include a reason(s) for the rejection of the Latent Fingerprint Image Search request.

3.4.8 Latent Fingerprint Feature Search

The Latent Fingerprint Feature Search request will contain fingerprint features and biographic descriptors. Fingerprint images may also be included in the feature search request if they are to be added to the Unsolved Latent File. Latent Fingerprint Image and Latent Fingerprint Feature Search requests are processed exactly the same except for the fact that IAFIS performs an automated feature extraction as part of Latent Fingerprint Image Search requests.

NGI-314

3.4.8.1 Latent Fingerprint Feature Search Inputs

SYS301 IAFIS (EFCON) shall accept Latent Fingerprint Feature Search requests from an Authorized Contributor via CJIS WAN.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

3.4.8.2 Latent Fingerprint Feature Search Processing

SYS302 IAFIS (AFIS) shall process Latent Fingerprint Feature Search requests in priority order.

SYS303 IAFIS (AFIS) shall support multiple priority levels for Latent Fingerprint Feature Search requests from state and local users.

Priorities will generally correspond to the following crime types:

- Homicide, rape, and special circumstances
- Kidnap, assault, and robbery
- Arson, drugs, personal crimes, and property crimes

Federal agencies will determine their own priority schemes. No additional validation of priorities will be provided. IAFIS will not interrupt searches in progress upon receipt of higher priority searches.

SYS304 IAFIS (AFIS) shall determine the percentage of file penetration based on the information provided in the Latent Fingerprint Feature Search request.

SYS305 IAFIS (AFIS) shall reject the Latent Fingerprint Feature Search when the percentage of file penetration exceeds the maximum allowable file penetration for the target repository.

SYS306 IAFIS (AFIS) shall provide the capability to treat multiple finger searches as a single Latent Fingerprint Feature Search request with a single file penetration percentage.

SYS307 IAFIS (AFIS) shall perform a feature quality check on a Latent Fingerprint Feature Search request based on quality standards.

SYS308 IAFIS (AFIS) shall reject a Latent Fingerprint Feature Search request when the features fail to satisfy minimum quality standards.

SYS309 IAFIS (AFIS) shall provide the capability to search using one or more fingers as part of a Latent Fingerprint Feature Search request.

SYS310 IAFIS (AFIS) shall utilize the Feature Search functionality when processing a Latent Fingerprint Feature Search request using the features provided on the request.

SYS311 IAFIS (AFIS) shall search the criminal fingerprint repository as part of a Latent Fingerprint Feature Search request from an Authorized Contributor.

Repositories that may be searched include the CMF, CIVIL, and any of the allowable SLCs.

SYS312 IAFIS (AFIS) shall search using the finger position(s), fingerprint classification data, biographic data, and extracted features provided as part of a Latent Fingerprint Feature Search request.

IAFIS will search all finger positions when no fingerprint position is indicated and a single finger is provided. If multiple finger positions are included with a single finger, then IAFIS will search the finger against all of the positions provided. If multiple fingers are provided, then IAFIS requires that a unique finger position be included for each finger.

SYS313 IAFIS (III) shall process the Latent Fingerprint Feature Search candidate list according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS314 IAFIS (ITN/TPS) shall provide a ranked candidate list including names, FNUs, match scores, and matching finger positions as a result of the Latent Fingerprint Feature Search request.

IAFIS will return 20 candidate FNUs as the result of a Latent Fingerprint Feature Search request.

SYS315 IAFIS (ITN/TPS) shall utilize the ISRE retrieval functionality when retrieving images in support of a Latent Fingerprint Feature Search request.

SYS316 IAFIS (ITN/ISRE) shall retrieve the indicated number of images, with a default of one, and the associated information as part of a Latent Fingerprint Feature Search request.

SYS317 IAFIS (ITN/ISRE) shall retrieve the matching fingerprint image from the candidate ten-print records as part of a Latent Fingerprint Feature Search request.

SYS318 IAFIS (AFIS) shall enroll subject feature information into the ULF, when indicated, as a result of a Latent Fingerprint Feature Search request.

SYS319 IAFIS (ITN/ISRE) shall enroll subject image information into the ULF, when indicated, as a result of a Latent Fingerprint Feature Search request.

SYS320 IAFIS (AFIS) shall temporarily add the fingerprint characteristics and descriptive data to the ULF when the Latent Fingerprint Feature Search request includes the ULF add indication.

IAFIS (AFIS) will use all temporary records in subsequent searches of the ULF.

SYS321 IAFIS (AFIS) shall provide the capability to designate the appropriate ULF record as permanent when an "add confirm" message is received as part of a Latent Fingerprint Feature Search request.

3.4.8.3 Latent Fingerprint Feature Search Outputs

SYS322 IAFIS (EFCON) shall provide the appropriate Latent Fingerprint Feature Search response to the Authorized Contributor via the CJIS WAN.

SYS323 IAFIS shall include a reason(s) for the rejection of the Latent Fingerprint Feature Search request.

3.4.9 Unsolved Latent Search

The Unsolved Latent Search request is a directed search against the ULF. IAFIS will allow Ten-Print fingerprint data or latent data to be searched against the ULF.

3.4.9.1 Unsolved Latent Search Inputs

SYS324 IAFIS (ITN/LPS) shall accept Unsolved Latent Search requests from an Authorized FBI Service Provider via an IAFIS Workstation.

SYS325 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to scan fingerprint data to initiate an Unsolved Latent Search request.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

3.4.9.2 Unsolved Latent Search Processing

SYS326 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to manually extract features from scanned images as part of an Unsolved Latent Search request.

SYS327 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to request an automatic extract of features from scanned images as part of an Unsolved Latent Search request.

SYS328 IAFIS (ITN/LPS) shall allow an Authorized FBI Latent Service Provider to determine the latent search priority as part of a Unsolved Latent Search request.

SYS329 IAFIS (AFIS) shall process Unsolved Latent Search requests in priority order.

SYS330 IAFIS (AFIS) shall support multiple priority levels for Unsolved Latent Search requests from state and local users.

Priorities will generally correspond to the following crime types:

- Homicide, rape, and special circumstances
- Kidnap, assault, and robbery
- Arson, drugs, personal crimes, and property crimes

Federal agencies will determine their own priority schemes. No additional validation of priorities will be provided. IAFIS will not interrupt searches in progress upon receipt of higher priority searches.

SYS331 IAFIS (AFIS) shall perform a feature quality check on an Unsolved Latent Search request based on quality standards.

SYS332 IAFIS (AFIS) shall reject an Unsolved Latent Search request when the features fail to satisfy minimum quality standards.

SYS333 IAFIS (AFIS) shall provide the capability to search using one or more fingers as part of

an Unsolved Latent Search request.

SYS334 IAFIS (AFIS) shall utilize the Feature Search functionality when processing an Unsolved Latent Search request using the features provided on the request.

SYS335 IAFIS (AFIS) shall search the unsolved latent repository as part of an Unsolved Latent Search request.

SYS336 IAFIS (AFIS) shall search using the finger position(s), fingerprint classification data, biographic data, and extracted features provided as part of an Unsolved Latent Search request.

An Authorized FBI Service Provider can indicate which finger position to search against in the IAFIS repository. If the Unsolved Latent Search request contains a single fingerprint image, the Service Provider can indicate multiple finger positions to be searched. If no finger position is indicated, then all finger positions will be searched.

SYS337 IAFIS (ITN/TPS) shall provide a ranked candidate list containing zero or more candidates including SCNAs, match scores, and matching finger positions as a result of the Unsolved Latent Search request.

SYS338 IAFIS (ITN/TPS) shall utilize the ISRE retrieval functionality when retrieving images in support of an Unsolved Latent Search request.

SYS339 IAFIS (ITN/ISRE) shall retrieve the ULF candidate images and the associated information as part of an Unsolved Latent Search request.

SYS340 IAFIS (ITN/LPS) shall store the results of an Unsolved Latent Search request for the Authorized FBI Service Provider that initiated the search.

3.4.9.3 Unsolved Latent Search Request Outputs

SYS341 IAFIS (ITN/LPS) shall provide the appropriate Unsolved Latent Search response to the Authorized FBI Service Provider via the IAFIS Workstation.

SYS342 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to view the candidate list returned from the Unsolved Latent Search request via IAFIS Workstation.

SYS343 IAFIS (ITN/LPS) shall allow an Authorized FBI Service Provider to print the candidate list returned from the Unsolved Latent Search request via the IAFIS Workstation.

SYS344 IAFIS shall include a reason(s) for the rejection of the Unsolved Latent Search request.

3.4.10 Latent Search Status and Modification Request

Latent Search Status and Modification Request provides an Authorized Contributor or Authorized FBI Service Provider the ability to check the status of a latent search request, adjust priority, adjust search order, or cancel a previously submitted latent search(es) that is queued in IAFIS. If the Latent Search is already in process, the Latent Search Status and Modification request will be rejected.

3.4.10.1 Latent Search Status and Modification Request Inputs

SYS345 IAFIS (EFCON) shall accept Latent Search Status and Modification Requests from an Authorized Contributor via the CJIS WAN.

NGI-318

SYS346 IAFIS (ITN/LPS) shall allow an Authorized FBI Service Provider to submit Latent Search Status and Modification Requests via an IAFIS Workstation.

3.4.10.2 Latent Search Status and Modification Request Processing

SYS347 IAFIS (AFIS) shall retrieve the SCNA of the referenced Latent Search(es) and the estimated time(s) to complete the search(es) when a status request is indicated as part of the Latent Search Status and Modification Request.

This SCNA will be referred to for any subsequent search modifications, which can include reprioritization, reordering, or cancellation of searches. Reprioritization cannot be requested in the same message as either reordering or cancellation of searches, and should be requested if needed before reordering or cancellation. If the same message is used to both reorder and cancel searches, the entire reorder operation will be performed first, followed by the canceling operation. Therefore, if the canceled search date/time stamp is desired to be retained and exchanged with another search, the canceled search must be listed with the reordered searches as well as in the field listing searches to be canceled.

SYS348 IAFIS (AFIS) shall provide the capability to perform pending search reordering (at the same priority) prior to canceling searches if both directions are received in the same message.

SYS349 IAFIS (AFIS) shall cancel a pending latent search request when a cancel request is indicated as part of a Latent Search Status and Modification Request.

SYS350 IAFIS (AFIS) shall reprioritize pending latent search request(s) when a reprioritization request is indicated as part of a Latent Search Status and Modification Request.

SYS351 IAFIS (AFIS) shall reorder pending latent search request(s) when a reorder request is indicated as part of a Latent Search Status and Modification Request.

SYS352 IAFIS (AFIS) shall reject the Latent Search Status and Modification Request when a specified Latent Search is not found in the Latent Search queue.

3.4.10.3 Latent Search Status and Modification Request Outputs

SYS353 IAFIS (ITN/LPS) shall provide, in a priority ordered list, the AFIS Segment Control Number (SCNA) and an estimated time to completion for each of the searches queried as part of the Latent Search Status and Modification Request.

AFIS will include in the results of a Search Status and Modification request the following information for each search: (1) The identity of each requested search including ORI, case number and extension and SCNA; (2) The position of the search in relation to other searches by that contributor, (3) The estimated time to completion for each search, and (4) The priority for each search if changed.

SYS354 IAFIS (EFCON) shall provide an appropriate response to a Latent Search Status and Modification Request via the CJIS WAN.

SYS355 IAFIS (ITN/LPS) shall provide an appropriate Latent Search Status and Modification Request response to an Authorized FBI Service Provider via the IAFIS Workstation.

SYS356 IAFIS (ITN/LPS) shall include a reason(s) for the rejection of the Latent Search Status and Modification request.

3.4.11 Latent Repository Statistics Query

The Latent Repository Statistics Query request allows the user to receive a statistical representation, based on descriptive data, of a latent repository and is used in updating a user's statistical representation to be used in a penetration query.

3.4.11.1 Latent Repository Statistics Query Inputs

SYS357 IAFIS (EFCON) shall accept Latent Repository Statistics Query requests from Authorized Contributors via the CJIS WAN.

3.4.11.2 Latent Repository Statistics Query Processing

SYS358 IAFIS (AFIS) shall calculate a statistical representation of the descriptors in the Latent Cognizant File using the descriptive data provided in the Latent Repository Statistics Query request.

3.4.11.3 Latent Repository Statistics Query Outputs

SYS359 IAFIS (EFCON) shall provide an electronic response to a Latent Repository Statistics Query request via the CJIS WAN.

3.4.12 Comparison Fingerprint Image(s) Submission (CFS)

The Comparison Fingerprint Image(s) Submission (CFS) supports the comparison of provided Ten-Print fingerprint images or other known prints against the provided latent impressions associated with a case. The CFS is intended solely for FBI use (i.e., field offices, FBI investigators). The CFS may include all the fingerprints normally enclosed in a Ten-Print submission plus optional additional prints (e.g., palm prints), if applicable.

The submitted fingerprints and latent prints will be analyzed and compared by an Authorized FBI Service Provider (Latent Examiner). Fingerprints for several individuals must be sent as individual submissions. No electronic response is returned for this submission. The contributor will be manually notified of comparison results via telephone, mail, email or fax.

3.4.12.1 Comparison Fingerprint Image Submission Inputs

SYS360 IAFIS (EFCON) shall accept Comparison Fingerprint Image Submissions via the CJIS WAN.

The Comparison Fingerprint Image Submission request is limited to FBI staff (e.g., field offices).

3.4.12.2 Comparison Fingerprint Image Submission Processing

SYS361 IAFIS (ITN/LPS) shall require an Authorized FBI Service Provider to perform a manual Latent Fingerprint Image Compare for each set of subject prints provided against latent prints provided as part of a Comparison Fingerprint Image Submission.

NGI-320

SYS362 IAFIS (ITN/LPS) shall provide the capability for an authorized FBI Service Provider to

perform all latent actions against the images provided in the Comparison Fingerprint Image Submission.

3.4.12.3 Comparison Fingerprint Image Submission Outputs

IAFIS does not generate a response for Comparison Fingerprint Image Submissions other than a communication protocol level acknowledgement.

3.4.13 Major Case Image(s) Submission (MCS) Request

The Major Case Image Submission (MCS) provides for the submission of Ten-Print fingerprints plus additional images of the extreme tips, sides, and lower joints of the fingers, and surface and extreme sides of palms for possible use in comparisons for a case. The MCS is intended solely for FBI use in conjunction with a Latent Print Unit investigation. The submitted prints will be added to the Major Case Image File. No electronic response is returned for this request.

3.4.13.1 Major Case Image Submission Inputs

SYS363 IAFIS (EFCON) shall accept Major Case Image Submissions via the CJIS WAN.

The Major Case Image Submission request is limited to FBI staff (e.g., field offices).

3.4.13.2 Major Case Image Submission Processing

SYS364 IAFIS (ITN/LPS) shall provide the capability for the authorized FBI Service Provider to enroll the information provided in a Major Case Image Submission into the Major Case Print File.

SYS365 IAFIS (ITN/LPS) shall provide the capability for an authorized FBI Service Provider to perform all latent actions against the images provided in the Major Case Image Submission.

These latent actions are fully described in the Workstation section below.

3.4.13.3 Major Case Image Submission Outputs

IAFIS does not generate a response for Major Case Image Submission, other than a communication protocol level acknowledgement.

3.4.14 Evaluation Latent Fingerprint Submission Request

The Evaluation Latent Fingerprint Submission Request (ELR) contains sets of latent fingerprints and provides the capability for FBI field office personnel to have the FBI Latent Fingerprint Section (LFPS) consult on cases. The transaction will result in a reply (e.g., NAR) indicating the action to be taken, which could include the establishment of a latent case, a request for additional information, or an evaluation of the case feasibility and recommendations for further actions. The FBI LFPS will be responsible for contacting the Authorized Contributor (FBI field office) with the results, which may include the establishment of a latent case, a request for additional information, or an evaluation of the case feasibility and recommendations for further actions.

3.4.14.1 Evaluation Latent Fingerprint Submission Request Inputs

SYS366 IAFIS (EFCON) shall accept Evaluation Latent Fingerprint Submission Requests via the CJIS WAN.

The Evaluation Latent Fingerprint Submission request is limited to FBI staff (e.g., field offices).

3.4.14.2 Evaluation Latent Fingerprint Submission Request Processing

SYS367 IAFIS (ITN/LPS) shall provide the capability for an authorized FBI Service Provider to perform all latent actions against the images provided in the Evaluation Latent Fingerprint Submission Request.

Evaluation Latent Fingerprint Submission Requests will be searched first against the criminal file. If no identification is made, the Evaluation Latent Fingerprint Submission Request may then be searched against other IAFIS repositories (i.e., civil, Special Latent Cognizant, ULF).

SYS368 IAFIS (ITN/LPS) shall allow Authorized FBI Latent Service Provider to enroll subject information into the designated IAFIS repository as a result of an Evaluation Latent Fingerprint Submission Request.

The allowable repositories to enroll the information are the ULF and SLC(s).

SYS369 IAFIS (ITN/LPS) shall reject an Evaluation Latent Fingerprint Submission Request if the submission indicates incorrect information or lack of mandatory data.

3.4.14.3 Evaluation Latent Fingerprint Submission Request Outputs

SYS370 IAFIS (EFCON) shall provide an appropriate response to an Evaluation Latent Fingerprint Submission Request via the CJIS WAN.

SYS371 IAFIS (ITN/LPS) shall include a reason(s) for the rejection of an Evaluation Latent Fingerprint Submission request.

IAFIS does not generate a response for Evaluation Latent Fingerprint Submission requests, other than a communication protocol level acknowledgement. The FBI Latent Service Provider who processes the transactions will be responsible for contacting the Authorized Contributor (FBI field office) with evaluation results.

3.5 Notification Services Functional Requirements

The Notification Service provides Authorized Contributors with unsolicited notifications from the system based on event criteria (triggers). An unsolicited notification may be triggered by functions initiated by the system, FBI Service Providers, or Authorized Contributors. The notifications to the users may be in multiple formats (e.g., electronic, telephonic, hardcopy).

The following section contains the functional requirements supporting IAFIS Notification User Services.

SYS372 IAFIS (III) shall be capable of sending unsolicited notifications to ITN printers.

The unsolicited notifications received from III will include: 1) Hit on Wanted/Missing Person Report, 2) Hit on Protected Witness/Quality Control Report, 3) Research and Advise Report, and 4) Multiple FNU for SID Report. The first two reports will be used to support Answer Hits to Wants and document processing. The last two reports will be used by the III Support Staff and Software Support Group.

SYS373 IAFIS (III) shall provide the capability to send unsolicited messages via NCIC.

SYS374 IAFIS (III) shall support the unsolicited messages described in III/NFF Operational and Technical Manual.

3.5.1 Flash Notifications

A Flash Notification will be provided to an Authorized Contributor when criminal activity or file maintenance occurs on a subject's record containing a Flash for that Contributor. Flashes may be placed on records for a subject whose activities are limited by court issued restrictions, supervision, protection orders, or deportation decrees.

SYS375 IAFIS (III) shall notify the originator of the flash when criminal activity occurs on a subject's record containing flash data.

SYS376 IAFIS (III) shall notify the originator of the flash when file maintenance occurs on a subject's record containing flash data.

SYS377 IAFIS (III) shall generate a hardcopy Subject Criminal History Rap Sheet for a Flash Notification.

SYS378 IAFIS (III) shall include the FBI Number and triggering event information in all Flash Notifications.

3.5.2 Want Notifications

A Wanted Persons Notification will be provided to an Authorized Contributor when activity or file maintenance occurs on a subject's record containing a Want Notice for that Contributor. Wants are placed on a subject when a Wanted Person is entered into NCIC with valid FBI Number. An FBI Service Provider may also place wants on a subject's record on behalf of an Authorized Contributor.

SYS379 IAFIS (III) shall notify the originator of a want when activity occurs on a subject's record containing want data.

SYS380 IAFIS (III) shall notify the originator of a want when file maintenance occurs on a subject's record containing want data.

SYS381 IAFIS (III) shall notify the originator of the want when processing a Criminal Print Identification message from an NFF State for a subject whose record contains a want.

SYS382 IAFIS (III) shall generate a hardcopy Subject Criminal History Rap Sheet for a Want Notification when appropriate.

SYS383 IAFIS (III) shall send a Want Notification to the originator of an Identification search, when the search results in a positive identification to a record containing want data.

SYS384 IAFIS (III) shall send Want Notifications as Nlets Administrative (AM) messages via

NCIC.

SYS385 IAFIS (III) shall include the FBI Number, subject biographic information, and triggering event information in all Want Notifications.

SYS386 IAFIS (III) shall send Hardcopy Want Notifications to Authorized FBI Service Providers.

3.5.3 Sexual Offender Registry Notifications

IAFIS will notify the original registering agency of activity on criminal subject records that contain Sexual Offender Registry (SOR) data. When there is file maintenance on a subject's record (e.g., posting an arrest, consolidating records, expungement of last cycle), IAFIS will send a notice to each registering agency.

SYS387 IAFIS (III) shall notify the registering agency when activity occurs on a subject's record containing Sexual Offender Registry data.

SYS388 IAFIS (III) shall notify the registering agency when file maintenance occurs on a subject's record containing Sexual Offender Registry data.

SYS389 IAFIS (III) shall send SOR Notifications as Nlets Administrative (AM) messages via NCIC.

SYS390 IAFIS (III) shall include the FBI Number, subject biographic information, and triggering event information in all SOR Notifications.

3.5.4 U.S. Marshall's Service Notifications

IAFIS will notify the U.S. Marshall's Service using a U.S Marshall Notification (USM) of activity on subjects marked for special interest. When there is file maintenance on a subject's record (e.g., posting an arrest, consolidating records, dispositions, expungement of last cycle), IAFIS will send a USM Notification.

SYS391 IAFIS (III) shall send a USM Notification when new arrest activity occurs on a subject for which they have a special interest.

SYS392 IAFIS (III) shall send a USM Notification when File Maintenance occurs on a subject for which they have a special interest.

SYS393 IAFIS (III) shall send a USM Notification when a subject for which they have a special interest is disseminated.

SYS394 IAFIS (III) shall send a USM Notification via the NCIC.

3.5.5 Other Special Interest Subject Notifications

IAFIS will notify the appropriate agency of activity on subjects of Special Interest. When there is file maintenance on a subject's record (e.g., posting an arrest, consolidating records, dispositions, expungement of last cycle), IAFIS will send a notice to the appropriate agency.

SYS395 IAFIS (III) shall send notifications to federal, state, and local agencies of criminal activity on persons who are of special interest by any such agency.

SYS396 IAFIS (III) shall route notifications of file maintenance on persons of special interest to authorized FBI Service Providers (via ITN).

SYS397 IAFIS (III) shall generate a hardcopy Special Interest Notification when appropriate.

3.5.6 III/NFF File Maintenance Notifications

A State Bureau for a III/NFF state will be notified when file maintenance activities (e.g., posting an arrest, consolidating records, or expungement of last cycle) occur against a record they own within IAFIS. Additionally, a III/NFF State Bureau will be notified of the search and record status resulting from a Ten-Print Fingerprint Identification Search submitted by an Authorized Contributor within their state.

SYS398 IAFIS (III) shall deliver unsolicited NCIC messages based on the IIIRES value associated with the ORI in the CCA file.

SYS399 IAFIS (III) shall send a Single-State Offender unsolicited message ($.A.SSO) to a III/NFF state when the status of a record changes from multi-source to single-source due to file maintenance activity.

SYS400 IAFIS (III) shall send a Multi-State Offender unsolicited message ($.A.MSO) to a III/NFF state when the status of a record changes from single-source to multi-source due to file maintenance activity.

SYS401 IAFIS (III) shall use the presence of SOR data as criteria for determining whether the III record is reported as having Single State Offender Status or a Multiple State Offender Status.

SYS402 IAFIS (III) shall send a Non-matching SID Ignored unsolicited message ($.A.NMS) to the submitting state when the SID on a new submission does not match the currently established SID on the identified record.

SYS403 IAFIS (III) shall send an Expunge record unsolicited message ($.A.EXP) to a III/NFF state when the last arrest is expunged from a record, resulting in the entire record being expunged.

SYS404 IAFIS (III) shall send an Expunge SID unsolicited message ($.A.EXS) to a III/NFF state when the last arrest for that state is expunged from a record and the record remains active.

SYS405 IAFIS (III) shall send a Consolidation unsolicited message ($.A.CON) to a III/NFF state when a record containing a SID for that state is involved in a Consolidation.

SYS406 IAFIS (III) shall send a Previously Established Record - Single Source unsolicited message ($.A.PES) to a NFF state when a subsequent arrest is received from that state for an individual and the record is single-source.

SYS407 IAFIS (III) shall send a Previously Established Record - Multi Source unsolicited message ($.A.PEM) to a NFF state when a subsequent arrest is received from that state for an individual and the record is multi-source.

SYS408 IAFIS (III) shall send a Deceased unsolicited message ($.A.DEC) to a III/NFF state when a record is marked as deceased and contains a SID for that state.

SYS409 IAFIS (III) shall send a SID Reactivated unsolicited message ($.A.REA) to the state whose SID was to be expunged to notify the state that their record is being reactivated when III reactivates "expungement pending" information.

NGI-325

SYS410 IAFIS (III) shall send a No Prior Record – Civil ($.A.CFN) unsolicited message to a III/NFF state when a Civil Ten-Print Fingerprint Identification Search from that state results in a non-identification decision.

SYS411 IAFIS (III) shall send a Prior Record – Civil ($.A.CFR) unsolicited message to a III/NFF state when a Civil Ten-Print Fingerprint Identification Search from that state results in an identification decision.

SYS412 IAFIS (III) shall send a No Prior Record – SID Entered ($.A.NPR) unsolicited message to a III/NFF state when a Criminal Ten-Print Fingerprint Identification Search from that state results in a non-identification decision, and the SID is added to the record.

SYS413 IAFIS (III) shall send a Prior Record – SID Entered ($.A.PIR) unsolicited message to a III/NFF state when a Criminal Ten-Print Fingerprint Identification Search from that state results in an identification decision, it is the first arrest for that state, and the SID is added to the record.

SYS414 IAFIS (III) shall send a Reject, No Prior Record, SID Not Entered ($.A.RNP) unsolicited message to a III/NFF state when a Criminal Ten-Print Fingerprint Identification Search from that state results in a non-identification decision and the SID cannot be added to the record.

SYS415 IAFIS (III) shall send a Reject, Prior Record, SID Not Entered ($.A.RPR) unsolicited message to a III/NFF state when a Criminal Ten-Print Fingerprint Identification Search from that state results in an identification decision, it is the first arrest for that state, and the SID cannot be added to the record.

SYS416 IAFIS (III) shall apply response generation rules to all III/NFF File Maintenance Notifications.

3.5.7 Unsolved Latent Match Notifications

The Unsolved Latent Match Notification informs the Unsolved Latent File (ULF) record owner that a potential match has occurred as a result of a Cascaded Fingerprint Search from a fingerprint transaction.

SYS417 IAFIS (EFCON) shall provide Unsolved Latent Match Notifications to Authorized Contributor via the CJIS WAN.

SYS418 IAFIS (ITN/LPS) shall provide an Unsolved Latent Match Notification to an Authorized FBI Service provider via the IAFIS Workstation.

3.5.8 Unsolicited Unsolved Latent Record Delete Notifications

The Unsolicited Unsolved Latent Record Delete Notification informs the Unsolved Latent File (ULF) record owner that their record has been deleted due to ULF reaching maximum capacity.

SYS419 AFIS shall provide an Unsolved Latent Record Deletion Notification to III when a ULF record owned by an Authorized Contributor is deleted as a result of the ULF reaching maximum capacity when a new record is being added to the ULF.

SYS420 AFIS shall provide an Unsolved Latent Match Notification to ITN/LPS when a ULF record owned by an Authorized FBI Service Provider is deleted as a result of the ULF reaching maximum capacity when a new record is being added to the ULF.

SYS421 IAFIS (EFCON) shall send Unsolicited Unsolved Latent Record Delete Notifications via the CJIS WAN.

SYS422 IAFIS (ITN/LPS) shall provide an Unsolicited Unsolved Latent Record Delete Notification to an Authorized FBI Service Provider.

3.5.9 Shared Data Notification

The Shared Data Notification Service provides Authorized Contributors with unsolicited notifications on event criteria (triggers). Shared Data Notifications are unsolicited messages between IAFIS (iDSM) and the IDENT system notifying the other agency of a positive identification.

SYS2175 IAFIS (iDSM) shall send a Shared Data Hit Notification to IDENT when there is a positive identification against an image contained in the IDENT shared data as a result of an Ten-Print Identification Search request from an Authorized iDSM Pilot Agency.

SYS2176 IAFIS (iDSM) shall include in the Shared Data Hit Notification to IDENT the associated IAFIS submission type (e.g., criminal arrest, civil application) that resulted in a positive identification against the IDENT shared data.

SYS2177 IAFIS (iDSM) shall include in the Shared Data Hit Notification to IDENT the associated Pilot Site Identifier for any IAFIS Ten-Print Identification Search request of the IDENT shared data resulting in a positive identification.

SYS2178 IAFIS (iDSM) shall accept a Shared Data Hit Notification from IDENT when there is a positive identification of a fingerprint submission against an image contained in the IAFIS Shared Data.

SYS2179 IAFIS (iDSM) shall accept as part of a Shared Data Hit Notification the reason for the IDENT submission type (e.g., Port of Entry (POE), Customs and Border Protection (CBP), Visa, Latent Search) that resulted in a positive identification.

SYS2180 IAFIS (iDSM) shall send Shared Data Hit Notifications via the CJIS WAN.

3.6 Data Management Service Functional Requirements

The following section contains the functional requirements supporting IAFIS Data Management User Services.

3.6.1 Fingerprint Image Replacement Request

A Fingerprint Image Replacement Request is a full replacement of composite fingerprint images and features. This service is only available for the Criminal Master File.

3.6.1.1 Fingerprint Image Replacement Request Inputs

SYS423 IAFIS (EFCON) shall accept Fingerprint Image Replacement Requests from Authorized Contributors via the CJIS WAN. NGI-327

SYS424 IAFIS (ITN/DPS) shall accept a Fingerprint Image Replacement Request via the IAFIS Workstation.

3.6.1.2 Fingerprint Image Replacement Request Processing

SYS425 IAFIS (ITN/ISRE) shall retrieve the fingerprint images from the FIMF associated with the specified FNU as part of a Fingerprint Image Replacement Request.

SYS426 IAFIS (ITN/ISRE) shall reject the Fingerprint Image Replacement Request when the specified FNU is invalid.

SYS427 IAFIS (ITN/TPS) shall require two Authorized FBI Service Providers to perform manual FICs for a Fingerprint Image Replacement Request.

SYS428 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to reject a Fingerprint Image Replacement Request as a result of the manual FIC.

SYS429 IAFIS (ITN/ISRE) shall update composite fingerprint images in the FIMF for the specified FNU using the fingerprint images provided in the Fingerprint Image Replacement Request.

SYS430 IAFIS (AFIS) shall update composite fingerprint features in the CMF repository for the specified FNU using the extracted fingerprint features of the fingerprint images provided in the Fingerprint Image Replacement Request.

SYS431 IAFIS (ITN/TPS) shall include a reason(s) for the rejection in the Fingerprint Image Replace Request response, when the request is unsuccessful.

SYS432 IAFIS (AFIS) shall cascade a fingerprint search of the ULF when a successful update of the composite fingerprint features is complete as a part of the Fingerprint Image Replace Request.

3.6.1.3 Fingerprint Image Replacement Request Outputs

SYS433 IAFIS (EFCON) shall provide a response to a Fingerprint Image Replacement Request via the CJIS WAN.

SYS434 IAFIS (ITN/DPS) shall provide the appropriate Fingerprint Image Replacement Request response via the IAFIS Workstation.

3.6.2 Subject Criminal History Record Modification Request

Subject Criminal History (SCH) Record Modification (SCHMOD) Request provides the capabilities for an Authorized Service Provider to modify subject criminal history information. This capability will allow the addition, modification, and deletion of selected data elements or criminal history events.

3.6.2.1 Subject Criminal History Record Modification Request Inputs

SYS435 IAFIS (ITN/DPS) shall accept a Subject Criminal History Record Modification Request via an IAFIS Workstation.

3.6.2.2 Subject Criminal History Record Modification Request Processing

NGI-328

SYS436 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History

Record for a provided FNU as part as of a Subject Criminal History Record Modification Request.

SYS437 IAFIS (ITN/DPS) shall send the designated maintenance action on the specified subject's criminal history record as part of the Subject Criminal History Record Modification Request (to III).

SYS438 IAFIS (III) shall process the Subject Criminal History Record Modification request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS439 IAFIS (III) shall reject the Subject Criminal History Record Modification Request when specified subject identifier is invalid.

SYS440 IAFIS (III) shall reject the Subject Criminal History Record Modification Request when the information in the request is invalid.

SYS441 IAFIS (III) shall perform the designated maintenance action as part of the Subject Criminal History Modification Request.

SYS442 IAFIS (ITN/DPS) shall accept a response to the Subject Criminal History Record Modification Request (from III).

SYS443 IAFIS (ITN/DPS) shall send an Update Descriptive Data Request (to AFIS) if changes occur to a subject's descriptive data.

SYS444 IAFIS (ITN/DPS) shall send a Delete FNU Request to ITN/ISRE when a subject deletion occurs.

SYS445 IAFIS (ITN/DPS) shall send a Delete FNU Request to ITN/ISRE when an old FNU is changed to a new FNU.

SYS446 IAFIS (ITN/DPS) shall send a Delete Fingerprint Features Request (to AFIS) when a subject deletion occurs.

SYS447 IAFIS (ITN/DPS) shall send a Delete Fingerprint Features Request (to AFIS) when an old FNU is changed to a new FNU.

SYS448 IAFIS (III) shall provide the capability to restore, to the previous state, all data for an FNU for up to 30 days after a record is deleted.

3.6.2.3 Subject Criminal History Record Modification Request Outputs

SYS449 IAFIS (ITN/DPS) shall provide the appropriate Subject Criminal History Record Modification Request response to an Authorized FBI Service Provider via the IAFIS Workstation.

3.6.3 III Record Maintenance Request

III Record Maintenance Request provides the capabilities for an Authorized Contributor to modify Subject Criminal History information. This capability will allow the addition, modification, and deletion of selected data elements.

3.6.3.1 III Record Maintenance Request Inputs

SYS450 IAFIS (III) shall accept a III Record Maintenance Request from an Authorized Contributor via NCIC.

The EHN III message supports the capability to add supplemental SCH biographic identifiers to specified subject and the capability to seal arrest records related to a specific state. The XHN III message supports the capability to delete supplemental SCH biographic identifiers from the specified subject. The MRS III message supports the capability to modify the III pointer data for the specified subject.

3.6.3.2 III Record Maintenance Request Processing

SYS451 IAFIS (III) shall perform the designated maintenance action on the specified subject's criminal history record as part of the III Record Maintenance Request.

SYS452 IAFIS (III) shall reject the III Record Maintenance Request when the specified subject identifier is invalid.

SYS453 IAFIS (III) shall reject the III Record Maintenance Request when the maintenance action is unsuccessful.

3.6.3.3 III Record Maintenance Request Outputs

SYS454 IAFIS (III) shall provide the appropriate III Record Maintenance Request response to an Authorized Contributor via NCIC.

SYS455 IAFIS (III) shall provide a reason(s) for rejection of the III Record Maintenance Request.

3.6.4 Special Stops Maintenance Request

The Special Stops Maintenance Requests provides the capability for an Authorized Service Provider to change SCH record status or permissions. This capability also allows an Authorized Service Provider to create SCH records with or without associated fingerprint image data.

3.6.4.1 Special Stops Maintenance Request Inputs

SYS456 IAFIS (ITN/DPS) shall accept a Special Stops Maintenance Request via the IAFIS Workstation.

Maintenance actions may include creation and deletions of records, along with modifications of audit (AUD) codes (i.e., AUD T to AUD P, AUD P to AUD T).

SYS457 IAFIS (ITN/DPS) shall allow an Authorized FBI Service Provider to scan fingerprint images as part of a Special Stops Maintenance Request when applicable.

The modification of a records AUD code from AUD T to AUD P will require the scanning of fingerprints.

3.6.4.2 Special Stops Maintenance Request Processing

SYS458 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of a Special Stops Maintenance Request.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS459 IAFIS (ITN/DPS) shall send the designated maintenance action on the specified subject's criminal history record as part of a Special Stops Maintenance Request (to III).

SYS460 IAFIS (III) shall process the Special Stops Maintenance request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS461 IAFIS (III) shall add a subject to the Criminal History File repository as part of an Add Special Stops Maintenance Request.

SYS462 IAFIS (ITN/ISRE) shall add fingerprint images to the FIMF repository as part of an Add Special Stops Maintenance Request.

SYS463 IAFIS (AFIS) shall add fingerprint features to the CMF repository as part of an Add Special Stops Maintenance Request.

Criminal records will be established using one of two scenarios. First, a Service Provider may scan in a ten-print card using the desktop scanner and then enter identification and arrest data in order to establish a subject criminal history record. The Service Provider may also enter court, additional court, and custody/supervisory-status data. Second, a Service Provider can create a criminal record by manually extracting the images of any ten fingers from existing image records in the FIMF and assembling the images to create a unique, composite fingerprint card which can then be used to create the special stops criminal record. The Service Provider will then enter identification and arrest data which may also contain court, additional court, and custody/supervisory-status data in order to establish a subject criminal history record as in the first scenario. The second scenario represents the fabrication of data.

SYS464 IAFIS (ITN/DPS) shall have the capability to designate the FBI Number to be assigned to a criminal record.

SYS465 IAFIS (III) shall reject the Special Stops Maintenance Request when the specified subject identifier is invalid.

SYS466 IAFIS (III) shall reject the Special Stops Maintenance Request when the information in the maintenance request is invalid.

SYS467 IAFIS (III) shall reject the Special Stops Maintenance Request when the maintenance action is unsuccessful.

3.6.4.3 Special Stops Maintenance Request Outputs

SYS468 IAFIS (III) shall include a reason(s) for rejection of the Special Stops Maintenance Request in the response.

SYS469 IAFIS (ITN/DPS) shall provide the appropriate Special Stops Maintenance Request response to an Authorized FBI Service Provider via the IAFIS Workstation.

NGI-331

3.6.5 Master SCH Record Conversion Request

Master SCH Record Conversion Request provides capability for Authorized Service Provider to add event and corresponding fingerprint image data to an existing SCH record marked as a manual record.

3.6.5.1 Master SCH Record Conversion Request Inputs

SYS470 IAFIS (ITN/DPS) shall accept a Master SCH Record Conversion Request via the IAFIS Workstation.

SYS471 IAFIS (ITN/DPS) shall allow an Authorized FBI Service Provider to scan fingerprint images as part of a Master SCH Record Conversion Request when applicable.

3.6.5.2 Master SCH Record Conversion Request Processing

SYS472 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of a Master SCH Record Conversion Request.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS473 IAFIS (ITN/DPS) shall send fingerprint image data to ITN/ISRE to be added to the FIMF repository as part of a Master SCH Record Conversion Request.

SYS474 IAFIS (ITN/DPS) shall send the criminal history event information to (III) Criminal History File repository for the specified subject identifier's record as part of a Master SCH Record Conversion Request.

SYS475 IAFIS (ITN/DPS) shall send an Update Fingerprint Features Request to (AFIS) CMF repository to add a features record corresponding to a new FNU as part of a Master SCH Record Conversion Request.

SYS476 IAFIS (III) shall reject the Master SCH Record Conversion Request when the specified subject identifier is invalid.

SYS477 IAFIS (III) shall reject the Master SCH Record Conversion Request when the information included in the request is invalid.

SYS478 IAFIS (III) shall reject the Master SCH Record Conversion Request when the update action is unsuccessful.

3.6.5.3 Master SCH Record Conversion Request Outputs

SYS479 IAFIS (III) shall include the reason(s) for rejection of the Master SCH Record Conversion Response.

SYS480 IAFIS (ITN/DPS) shall provide the appropriate Master SCH Record Conversion Request response to an Authorized FBI Service Provider via the IAFIS Workstation.

3.6.6 Disposition Submission

The Disposition Submission service updates a criminal history record by associating court and custody information to an arrest cycle. Disposition processing submissions may be on paper or machine readable data (MRD) media.

3.6.6.1 Disposition Submission Inputs

SYS481 IAFIS (III) shall accept a Disposition Submission request from Authorized Contributors via the MRD process.

SYS482 IAFIS (ITN/DPS) shall accept a Disposition Submission request via the IAFIS Workstation.

3.6.6.2 Disposition Submission Processing

SYS483 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of a Disposition Submission Request.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS484 IAFIS (ITN/DPS) shall send a request to update the (III) Criminal History File repository for the specified FNU and Date of Arrest using the data provided in the Disposition Submission request.

SYS485 IAFIS (III) shall process the Disposition Submission request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS486 IAFIS (ITN/DPS) shall send an add request to the (III) Criminal History File repository for the specified FNU and Date of Arrest using the data provided in the Disposition Submission request.

SYS487 IAFIS (III) shall reject a Disposition Submission request when the specified FNU is invalid.

SYS488 IAFIS (III) shall reject a Disposition Submission request when the specified DOA is invalid.

SYS489 IAFIS (III) shall reject a Disposition Submission request when the update action is unsuccessful.

SYS490 IAFIS (III) shall suspend file maintenance and send an error notification message (to ITN) when the Disposition Submission request attempts to update a criminal history record that contains a Bureau Fugitive want and the Service Provider is not specifically authorized to process Bureau Fugitive want information.

SYS491 IAFIS (ITN/DPS) shall send the error notification to an Authorized FBI Service Provider via the IAFIS Workstation as part of the Disposition Submission Request.

SYS492 IAFIS (III) shall require a subject criminal history record that contains a Bureau Fugitive want(s) with a pending dispositional file maintenance request to be reviewed by an Authorized FBI Service Provider who is specifically authorized to process records with Bureau

Fugitive want information.

SYS493 IAFIS (III) shall print the disposition and criminal history information (for Service Provider review) when the potential disposition data will update a criminal history record that contains a Bureau Fugitive want and the disposition transaction was received via the MRD process.

SYS494 IAFIS (III) shall print Bureau Fugitive related disposition and criminal history information to the ITN/DPS want/flash printer located in the Want/Flash processing area.

3.6.6.3 Disposition Submission Outputs

SYS495 IAFIS (III) shall provide an MRD response to a Disposition Submission request via the MRD process.

SYS496 IAFIS (ITN/DPS) shall provide the appropriate Disposition Submission response to an Authorized FBI Service Provider via the IAFIS Workstation.

3.6.7 NCIC Expungement Submission

The Expungement Submission request removes criminal history data for a specified arrest. Specific charges may be expunged from an arrest or an entire arrest may be expunged. If the last arrest on a criminal history record is expunged, then the entire record will be expunged.

3.6.7.1 NCIC Expungement Submission Inputs

SYS497 IAFIS (III) shall accept electronic Expungement Submission requests from Authorized Contributors via NCIC.

3.6.7.2 NCIC Expungement Submission Processing

SYS498 IAFIS (III) shall process the NCIC Expungement Submission request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS499 IAFIS (III) shall temporarily expunge all criminal history data associated with the expungement request received via NCIC.

SYS500 IAFIS (III) shall restore criminal history data that remains in the temporarily expunged state for more than 30 days after the completion of an electronic NCIC Expungement Submission request from a non-NFF state.

The non-NFF expungement request will need to be followed with a hardcopy expungement request from the contributor to permanently expunge the specific arrest information.

SYS501 IAFIS (III) shall permanently expunge criminal history data that remains in the temporarily expunged stat for more than 1 hour after the completion of an electronic NCIC Expungement Submission request from an NFF state.

The expungement can be reversed by the NFF state within 1 hour of the initial expungement request via the MRS III Record Maintenance request.

IAFIS (III) will send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the record being expunged.

NGI-334

SYS502 IAFIS (III) shall reject an NCIC Expungement Submission request when the specified FNU or SID is invalid.

SYS503 IAFIS (III) shall reject the NCIC Expungement Submission request if the expungement action is unsuccessful.

3.6.7.3 NCIC Expungement Submission Outputs

SYS504 IAFIS (III) shall provide an NCIC response to an Expungement Submission request received via the NCIC.

SYS505 IAFIS (III) shall include the reason(s) for rejection of the NCIC Expungement Submission request.

3.6.8 Non-NCIC Expungement Submission

The Expungement Submission request removes criminal history data for a specified arrest. Specific charges may be expunged from an arrest or an entire arrest may be expunged. If the last arrest on a criminal history record is expunged, then the entire record will be expunged.

3.6.8.1 Non-NCIC Expungement Submission Inputs

SYS506 IAFIS (III) shall accept Expungement Submission requests from Authorized Contributors via the MRD process.

SYS507 IAFIS (ITN/DPS) shall accept an Expungement Submission request via the IAFIS Workstation.

SYS508 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to expunge one or more charges from an existing arrest.

A partial expungement is the removal of at least one, but not all, of the charges associated with a particular arrest.

SYS509 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to expunge an entire existing arrest.

A cycle expungement is the removal of all charges associated with a particular arrest.

3.6.8.2 Non-NCIC Expungement Submission Processing

SYS510 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of an Expungement Submission Request via the IAFIS Workstation.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS511 IAFIS shall expunge the arrest data and appropriate criminal history information associated with the FNU and Date of Arrest provided in the Non-NCIC Expungement Submission request.

SYS512 IAFIS (III) shall process the Expungement Submission request according to the IAFIS

ICD when the criminal history record contains a Special Processing Flag(s).

IAFIS will finalize an electronic DRS expungement previously processed by III by posting the follow-up hardcopy to the subject's record.

SYS513 IAFIS (III) shall permanently expunge data that was marked as temporarily expunged by a previous NCIC Expungement Submission request from a non-NFF state when a Non-NCIC Expungement Submission request is processed.

SYS514 IAFIS (ITN/DPS) shall perform a criminal record expungement when the last arrest is expunged.

If the expungement is for a single remaining arrest cycle in the subject's file, III will determine if there is an outstanding want on the subject recorded in the III files. If no want is outstanding, III will notify ITN to delete fingerprint features data. ITN will initiate delete/update requests to AFIS to purge the subject's records.

SYS515 IAFIS (III) shall provide the capability to restore, to the previous state, all data for an FNU for up to 30 days after a record is expunged.

SYS516 IAFIS (ITN/ISRE) shall remove images associated with the criminal record as a result of a criminal record expungement.

SYS517 IAFIS (AFIS) shall remove features associated with the criminal record as a result of a criminal record expungement.

IAFIS will not remove fingerprint images and features when a single arrest cycle is expunged, even if the images and features on the record were obtained from the fingerprint cycle that is being expunged.

IAFIS (III) will send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the record being expunged.

SYS518 IAFIS (III) shall reject a Non-NCIC Expungement Submission request when the specified FNU is invalid.

SYS519 IAFIS (III) shall reject a Non-NCIC Expungement Submission request when the specified DOA is invalid.

SYS520 IAFIS (III) shall reject the Non-NCIC Expungement Submission request if the expungement action is unsuccessful.

3.6.8.3 Non-NCIC Expungement Submission Outputs

SYS521 IAFIS (III) shall provide an MRD response to an Expungement Submission request received via the MRD process.

SYS522 IAFIS (ITN/DPS) shall provide the appropriate Non-NCIC Expungement response to an Authorized FBI Service Provider via the IAFIS Workstation.

SYS523 IAFIS (ITN/DPS) shall include the reason(s) for rejection of the Non-NCIC Expungement Submission request.

3.6.9 Criminal Record Sealing Request

Criminal Record Sealing Request allows an Authorized Contributor to restrict the access of the criminal history information associated with arrests that they own. The FBI will limit dissemination of criminal history data related to a sealed criminal arrest record. An FBI Service Provider can "seal" individual arrest records on behalf of an Authorized Contributor.

3.6.9.1 Criminal Record Sealing Request Inputs

SYS524 IAFIS (III) shall accept electronic Criminal Record Sealing Submission Requests Authorized Contributors via NCIC.

SYS525 IAFIS (ITN/DPS) shall accept a Criminal Record Sealing Request via the IAFIS Workstation.

3.6.9.2 Criminal Record Sealing Request Processing

SYS526 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of a Criminal Record Sealing Request via the IAFIS Workstation.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS527 IAFIS (III) shall seal a criminal arrest record and associated criminal history information when indicated in the Criminal Record Sealing Request.

SYS528 IAFIS (III) shall un-seal a criminal arrest record and associated criminal history information when indicated in the Criminal Record Sealing Request.

SYS529 IAFIS (III) shall process the Criminal Record Sealing Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS530 IAFIS (III) shall reject a Criminal Record Sealing Request when the specified FNU is invalid.

SYS531 IAFIS (III) shall reject a Criminal Record Sealing Request when the specified arrest record information is invalid.

SYS532 IAFIS (III) shall reject a Criminal Record Sealing Request when the file maintenance action is unsuccessful.

3.6.9.3 Criminal Record Sealing Request Outputs

SYS533 IAFIS (ITN/DPS) shall provide the appropriate Criminal Record Sealing Request response via the IAFIS Workstation.

SYS534 IAFIS (ITN/DPS) shall include the reason(s) for rejection of the Criminal Record Sealing Request.

3.6.10 Criminal Record Consolidation Request

A Criminal Record Consolidation Request will be initiated when multiple Subject Criminal History Records are found to exist for the same individual. A service provider will review the criminal fingerprint images and determine if the records should be consolidated. The Criminal Record Consolidation Request causes the information in the multiple records to be merged and the information associated with the secondary records to be deleted. As a result of the consolidation, a notification will be sent to the agency that submitted the fingerprints; any agencies that have submitted fingerprints pertinent to any of the records in the last year; and all state ID bureaus that have submitted fingerprints or records at any time on the consolidated subject.

3.6.10.1 Criminal Record Consolidation Request Inputs

SYS535 IAFIS (ITN/DPS) shall accept a Criminal Record Consolidation Request via the IAFIS Workstation.

This input is known as the 'Forward FNU' process.

SYS536 ITN/DPS shall accept a Criminal Record Consolidation Request from ITN/TPS when more than one criminal candidate from a Ten-Print Identification Search receives an Identification decision.

3.6.10.2 Criminal Record Consolidation Request Processing

The following requirements are part of the 'Forward FNU' processing:

SYS537 ITN/DPS shall forward FNUs to AFIS processing for III/Verify to confirm a possible consolidation.

SYS538 ITN/DPS shall forward FNUs to ITN/TPS processing for FIC processing to confirm a possible consolidation.

SYS539 IAFIS (ITN/DPS) shall retrieve images for possible consolidation via ITN/ISRE.

SYS540 IAFIS (ITN/ISRE) shall place the first FNU stated in the consolidation request into the 'submission' image and the remaining FNUs in the consolidation request as 'candidate' images.

SYS541 IAFIS (ITN/TPS) shall require two manual FIC comparisons for each candidate in the forwarded consolidation request.

SYS542 IAFIS (ITN/TPS) shall require EVAL to confirm each identification decision for the candidates in the forwarded consolidation request.

SYS543 IAFIS (ITN/TPS) shall reject a Criminal Record Consolidation Request when the fingerprints for the FNUs are determined to not be the same individual.

The following requirements are for both 'Forward FNU' and Ten-Print processing consolidations:

SYS544 IAFIS (ITN/TPS) shall forward the consolidation request through IAFIS Filtering rules when two or more FNUs are determined to be IDENT.

SYS545 ITN/TPS shall forward the consolidation request to III indicating automatic consolidation when the consolidation request passes IAFIS Filtering rules.

SYS546 IAFIS (III) shall designate the oldest FNU as the kept FNU and the remaining FNU(s) as the killed FNU(s) as part of a Criminal Record Consolidation Request.

SYS547 IAFIS (III) shall consolidate the criminal history information associated with the "killed FNU(s)" into the "kept FNU" (FBK) provided when none of the FNUs contain special processing flags or NFF data as part of the automated consolidation process.

SYS548 IAFIS (III) shall send the consolidation request to ITN/DPS when automatic consolidation cannot be performed by III.

SYS549 IAFIS (ITN/DPS) shall retrieve Subject Criminal History Records for each FNU for review by an Authorized FBI Service Provider as part of the manual consolidation process.

SYS550 IAFIS (ITN/DPS) shall allow an Authorized FBI Service Provider to determine "kept FNU" (FBK) and "killed FNU(s)" from the FNUs provided as part of the manual consolidation process.

SYS551 IAFIS (III) shall consolidate the criminal history information associated with the "killed FNU(s)" into the "kept FNU" (FBK) provided as part of the Manual Criminal Record Consolidation Request.

SYS552 IAFIS (III) shall process the Criminal Record Consolidation Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS553 IAFIS (III) shall provide the capability to restore, to the previous state, all data for an FNU for up to 30 days after a record is updated by a consolidation.

SYS554 IAFIS (III) shall reject a Criminal Record Consolidation Request when the consolidation action is unsuccessful.

SYS555 IAFIS (ITN/TPS) shall update the composite image based on image replacement decisions made during the fingerprint comparison process as part of the Criminal Record Consolidation Request.

SYS556 IAFIS (AFIS) shall update the composite feature set based on image replacement decisions made during the fingerprint comparison process as part of the Criminal Record Consolidation Request.

SYS557 IAFIS (III) shall apply the consolidation process to the associated criminal photo set stored in the Criminal Subject Photo File as part of a Criminal Record Consolidation.

3.6.10.3 Criminal Record Consolidation Request Outputs

SYS558 IAFIS (III) shall provide hardcopy Rap Sheets to each contributor that provided or received criminal history information for the kept FNU during the last 12-month time period.

IAFIS (III) will also send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the records being consolidated. Refer to the *Notification Services Functional Requirements* section for more information.

SYS559 IAFIS (ITN/DPS) shall provide the appropriate Criminal Record Consolidation request response to an Authorized FBI Service Provider via the IAFIS Workstation.

SYS560 IAFIS (ITN/DPS) shall include the reason(s) for rejection of the Criminal Record Consolidation Request.

NGI-339

Ten-Print Fingerprint Identification requests that trigger a Consolidation Request will resume normal processing after consolidation activities are completed.

3.6.11 Death Notice Request

A death notice differs from a Known Deceased submission in that the fingerprints on the fingerprint card submission are not required for this process. Any fingerprint card submitted with fingerprint impressions will be used for textual data entry only.

3.6.11.1 Death Notice Request Inputs

SYS561 IAFIS (III) shall accept a Death Notice Request from Authorized Contributors via NCIC.

3.6.11.2 Death Notice Request Processing

SYS562 IAFIS (III) shall update the specified FNU with information provided in a Death Notice Request.

SYS563 IAFIS (III) shall update a subject's record with "notice of death received" when a death notice request is received.

SYS564 IAFIS (III) shall process the Death Notice Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS565 IAFIS (III) shall provide the capability to restore, to the previous state, all data for an FNU for up to 30 days after a record is deceased.

SYS566 IAFIS (III) shall reject a Death Notice Request when the FNU is invalid.

3.6.11.3 Death Notice Request Outputs

SYS567 IAFIS (III) shall provide an appropriate response to a Death Notice Request via NCIC.

SYS568 IAFIS (III) shall include the reason(s) for rejection of the Death Notice Request.

IAFIS (III) will also send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the record being deceased. Refer to the *Notification Services Functional Requirements* section for more information.

3.6.12 Want Maintenance Request

Criminal Justice users can submit want notices to be entered into a subject's record in order to request that they be notified of the apprehension of that subject. IAFIS will receive want information electronically from NCIC. NCIC will transmit electronic want information to IAFIS in an electronic message.

IAFIS Want processing will be based upon III maintaining the Want information for IAFIS processing of transactions and preparation of responses. III will maintain its Want information from data received from the NCIC system and information entered by ITN/DPS Service Providers. III will provide Want information to requestors and will include Want information in III responses. IAFIS will notify the originator of the Want whenever IAFIS processes new arrest information or includes Want information in a criminal history response.

3.6.12.1 Want Maintenance Request Inputs

SYS569 IAFIS (III) shall accept Want Maintenance Requests from the NCIC system.

III will receive messages from NCIC whenever NCIC processes a Want transaction that has an assigned FBI Number. NCIC Want Messages will be identified by the Input Message Key field in Table 3.6.12-1. III will then perform the associated III file maintenance operation.

Table 3.6.12-1 NCIC Wanted Person Input Message Key Fields

Input Message Key	IAFIS Operations
EW	add Entered Want information; (*Note that these Message Keys may include Caution Indicator codes, such as in EW-C)
MW	update Want information with Modify data
XW	delete Want information
CW	processed as a delete of Want information
LW	processed as a delete of Want information

SYS570 IAFIS (ITN/DPS) shall accept Want Maintenance Requests via the IAFIS Workstation.

In order to enter other wants received without an FBI Number, ITN/DPS Service Providers will verify that the subject has a record in the SCH file, determine the correct FBI Number, and submit a file maintenance transaction to add the want information. If the subject is not in the SCH file and the want is not a Bureau Fugitive, it will be rejected by the Service Provider.

3.6.12.2 Want Maintenance Request Processing

SYS571 IAFIS (ITN/DPS) shall provide the capability of an Authorized FBI Service Provider to perform a Subject Search as part of the Want Maintenance process.

The FBI Service Provider will use the results of the Subject Search to verify the identity of the subject to which the want information is to be applied.

SYS572 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of a Want Maintenance Request.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS573 ITN/DPS shall send a Want Maintenance Request to III containing the appropriate criminal history information.

SYS574 IAFIS (III) shall update the Criminal History record for the associated FNU using the designated file maintenance type and other data contained in the Want Maintenance Request.

The want information maintained may include the following fields: date of entry, ORI or originator of warrant, date of warrant, and NCIC Number.

SYS575 IAFIS (III) shall process the Want Maintenance Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS576 IAFIS (III) shall be capable of storing an unlimited number of wants per subject.

Similar to the number of arrests allowed per subject, there has been no limit placed on the number of wants that can be submitted for each subject.

SYS577 IAFIS (III) shall reject a Want Maintenance Request when the specified FNU is invalid.

SYS578 IAFIS (III) shall reject a Want Maintenance Request when discrepancies exist between the incoming want data and the contents of the subject's record.

3.6.12.3 Want Maintenance Request Outputs

IAFIS does not provide any response when an NCIC Want Maintenance Request completes successfully.

SYS579 III shall send an appropriate reject message to an ITN printer in accordance with the IAFIS ICD in order to notify Authorized FBI Service Providers of a rejected Want Maintenance Request.

Service Providers will resolve the discrepancies through searches of the NCIC files (at an NCIC workstation) and IAFIS files (at an IAFIS workstation). The Service Provider will perform the Want Maintenance when all discrepancies are resolved.

SYS580 IAFIS (ITN/DPS) shall provide the appropriate Want Maintenance Request response to an Authorized FBI Service Provider when the request was initiated via the IAFIS Workstation.

SYS581 IAFIS (III) shall include the reason(s) for rejection of the Want Maintenance Request.

3.6.13 Flash Submission

IAFIS will receive flash information in hardcopy from criminal justice agencies. Want Service Providers will enter the flash information and submit file maintenance requests to add the flash information to a subject's SCH file record.

3.6.13.1 Flash Submission Inputs

SYS582 IAFIS (ITN/DPS) shall accept a Flash Submission from an Authorized FBI Service Provider via the IAFIS Workstation.

3.6.13.2 Flash Submission Processing

SYS583 IAFIS (ITN/DPS) shall provide the capability to access a Subject's Criminal History Record for a provided FNU as part as of a Flash Submission.

An authorized FBI Service Provider will have the ability to display the Subject's Criminal History prior to issuing the request and after the completion of the request to verify the request was completed.

SYS584 ITN/DPS shall send a Flash Submission to III containing the appropriate criminal history information.

SYS585 IAFIS (III) shall process the Flash Submission according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS586 IAFIS (III) shall update the Criminal History record for the associated FNU and DOA using the information contained in the Flash Submission.

The information maintained for each Flash Notice may include the following fields: ORI of agency to be notified, Originating Agency case number, date probation ends, and date start of supervision.

SYS587 IAFIS (III) shall reject a Flash Submission when the specified FNU is invalid.

SYS588 IAFIS (III) shall reject a Flash Submission when the specified DOA is invalid.

ITN/DPS Service Providers may enter flash data into a subject's record as a routine flash (SPF = F) or as a federal diversion probation (SPF = Q).

3.6.13.3 Flash Submission Request Outputs

SYS589 IAFIS (ITN/DPS) shall provide the appropriate Flash Submission response via the IAFIS Workstation.

SYS590 IAFIS (III) shall generate a hardcopy response to a Flash Submissions, if appropriate.

SYS591 IAFIS (III) shall include the reason(s) for rejection of the Flash Submission.

IAFIS (III) will also send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the record being updated. Refer to the *Notification Services System Requirements* section for more information.

3.6.14 Sexual Offender Registry (SOR) Maintenance Request

Electronic SOR Maintenance Requests are received from NCIC when sexual offender information is added, modified, or deleted within the NCIC sexual offender file and there is an FNU associated with the record. If IAFIS cannot automatically process the electronic Sexual Offender Registry Maintenance Request, a reject message is printed for an Authorized FBI Service Provider to review.

3.6.14.1 SOR Maintenance Request Inputs

SYS592 IAFIS (III) shall accept SOR Maintenance Requests from the NCIC system.

III will receive messages from NCIC whenever NCIC processes an SOR Maintenance transaction that has an assigned FBI Number. NCIC SOR Maintenance Messages will be identified by the Input Message Key field in Table 3.6.14-1. III will then perform the associated III file maintenance operation.

Table 3.6.14-1 NCIC Sexual Offender Registration Input Message Key Fields

MKE	IAFIS Operation
EXS	Enter Sexual Offender, will add SOR data to a subjects record.

EXSC	Enter Sexual Offender—Caution, processed the same as EXS.
MXS	Modify Sexual Offender, will modify requested SOR data fields in a subjects record.
XXS	Cancel Sexual Offender, will cause the requested SOR data to be physically deleted.
CXS	Clear Sexual Offender, will cause the requested SOR data to be physically deleted.

3.6.14.2 SOR Maintenance Request Processing

SYS593 IAFIS (III) shall process the SOR Maintenance Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS594 IAFIS (III) shall update the Criminal History record for the associated FNU using the designated file maintenance type and other data contained in the SOR Maintenance Request.

SYS595 IAFIS (III) shall add the subject's name, as an alias to the subject's identification data, if the name included in the received sexual offender registration data does not exist in the matching subject record.

SYS596 IAFIS (III) shall be capable of storing an unlimited number of sexual offender registrations per subject.

Similar to the number of arrests allowed per subject, there has been no limit placed on the number of registrations that can be submitted for each subject.

SYS597 IAFIS (III) shall reject an SOR Maintenance Request when the specified FNU is invalid.

SYS598 IAFIS (III) shall reject an SOR Maintenance Request when discrepancies exist between the incoming SOR data and the contents of the subject's record.

3.6.14.3 SOR Maintenance Request Outputs

SYS599 III shall send an appropriate reject message to an ITN printer in accordance with the IAFIS ICD in order to notify Authorized FBI Service Providers of a rejected Sexual Offender Notification.

Service Providers will resolve the discrepancies through searches of the NCIC files (at an NCIC workstation) and IAFIS files (at an IAFIS workstation), and phone calls to the registering agency. The Service Provider will inform the registering agency of the rejection and inform them of the necessary action to correct the problem. The registering agency will submit new SOR transactions to NCIC to correct the problem.

SYS600 IAFIS (III) shall include the reason(s) for rejection of the SOR Maintenance Request.

IAFIS (III) will also send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the record being updated. Refer to the *Notification Services System Requirements* section for more information.

3.6.15 Photo Image Delete Request

3.6.15.1 Photo Image Delete Request Inputs

SYS601 IAFIS (EFCON) shall accept Photo Image Delete Requests from Authorized Contributors via the CJIS WAN.

3.6.15.2 Photo Image Delete Request Processing

SYS602 IAFIS (III) shall process the Photo Image Delete Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS603 IAFIS (III/IPS) shall delete the photo set associated with the FNU and Date of Arrest (DOA) provided as part of a Photo Image Delete Request.

SYS604 IAFIS (III/IPS) shall update the photo summary information as part of photo deletion processing.

SYS605 IAFIS (III/IPS) shall reject a Photo Image Delete Request when the Contributor of the request is not the owner of the photo set.

SYS606 IAFIS (III/IPS) shall reject a Photo Image Delete Request when the specified FNU is invalid.

SYS607 IAFIS (III/IPS) shall reject a Photo Image Delete Request when the specified DOA does not exist in the record.

3.6.15.3 Photo Image Delete Request Outputs

SYS608 IAFIS (EFCON) shall provide an appropriate response to a Photo Image Delete Requestvia the CJIS WAN.

SYS609 IAFIS (III) shall include the reason(s) for rejection of the Photo Image Delete Request.

3.6.16 Unsolved Latent Add Confirm Request

This request is used to confirm temporarily added unsolved latent file records.

3.6.16.1 Unsolved Latent Add Confirm Inputs

SYS610 IAFIS (EFCON) shall accept Unsolved Latent Add Confirm request via the CJIS WAN.

SYS611 IAFIS (ITN/LPS) shall accept Unsolved Latent Add Confirm request via the IAFIS Workstation.

3.6.16.2 Unsolved Latent Add Confirm Processing

SYS612 IAFIS (ITN/ISRE) shall mark the appropriate ULF image record as permanent in the ULF repository as part of an Unsolved Latent Add Confirm request.

SYS613 IAFIS (AFIS) shall mark the appropriate ULF feature record as permanent in the ULF repository as part of an Unsolved Latent Add Confirm request.

NGI-345

3.6.16.3 Unsolved Latent Add Confirm Outputs

SYS614 IAFIS (EFCON) shall provide an appropriate response to the Unsolved Latent Add Confirm Request via CJIS WAN.

SYS615 IAFIS (ITN/LPS) shall provide the appropriate Unsolved Latent Add Confirm Request response to an Authorized FBI Service Provider via the IAFIS Workstation.

3.6.17 Unsolved Latent File (ULF) Delete Request

The Unsolved Latent File Delete Request provides the capability for a ULF record owner to delete a latent print from the ULF.

3.6.17.1 ULF Delete Request Inputs

SYS616 IAFIS (EFCON) shall accept Unsolved Latent File Delete Requests from an Authorized Contributor via the CJIS WAN.

SYS617 IAFIS (ITN/LPS) shall allow an Authorized FBI Service Provider to submit an Unsolved Latent File Delete Request via the IAFIS Workstation.

3.6.17.2 ULF Delete Request Processing

SYS618 IAFIS (AFIS) shall delete the fingerprint feature data from the Unsolved Latent File associated with the unique identifier specified in the Unsolved Latent File Delete Request.

SYS619 IAFIS (ITN/ISRE) shall delete the fingerprint image data from the Unsolved Latent File associated with the unique identifier specified in the Unsolved Latent File Delete Request.

SYS620 IAFIS (AFIS) shall reject an Unsolved Latent File Delete Request when the requestor is not the owner of the ULF record.

SYS621 IAFIS (AFIS) shall reject an Unsolved Latent File Delete Request when the specified unique identifier does not exist.

3.6.17.3 ULF Delete Request Outputs

SYS622 IAFIS (EFCON) shall provide an appropriate response to the Unsolved Latent Delete Request via CJIS WAN.

SYS623 IAFIS (ITN/LPS) shall provide the appropriate Unsolved Latent Delete Request response to an Authorized FBI Service Provider via the IAFIS Workstation.

SYS624 IAFIS (ITN) shall include the reason(s) for rejection of the Unsolved Latent Delete Request.

3.6.18 Special Latent Cognizant Record Maintenance Request

The Special Latent Cognizant Record Maintenance request provides the capability for an Authorized Contributor or FBI Service Provider (Latent Examiner) to maintain (add/copy/delete) data for a Special Latent Cognizant File.

3.6.18.1 Special Latent Cognizant Record Maintenance Request Inputs

The Card Scanning Service (CSS) will only be capable of performing an add as part of a Special Latent Cognizant Record Maintenance request.

SYS625 IAFIS (ITN/LPS) shall allow an Authorized FBI Service Provider to submit a Special Latent Cognizant Record Maintenance request via an IAFIS Workstation.

SYS626 IAFIS (ITN/LPS) shall allow an authorized FBI Service Provider to scan fingerprint data to initiate a Special Latent Cognizant Record Maintenance request.

IAFIS will support scanning all fingerprints at a sufficient density and resolution for fingerprint classification, feature extraction, and identification. The scanner output will be in accordance with the ANSI/NIST image transmission standard for fingerprint data "American National Standards Institute/National Institute of Standards and Technology standard, *Data Format for the Interchange of Fingerprint Information*" and with the EFTS.

3.6.18.2 Special Latent Cognizant Record Maintenance Request Processing

SYS627 IAFIS (ITN/LPS) shall provide the capability to add images, features, and text records using a list of FNU(s), CRN(s), or SCNA(s) as part of the Special Latent Cognizant Record Maintenance request.

SYS628 IAFIS (ITN/LPS) shall provide the capability to copy all records from one SLC file to another SLC file as part of the Special Latent Cognizant Record Maintenance request.

SYS629 IAFIS (ITN/LPS) shall provide the capability to modify the biographic data associated with a SLC record as part of the Special Latent Cognizant Record Maintenance request.

SYS630 IAFIS (ITN/LPS) shall provide the capability to delete a SLC record using an FNU, CRN, or SCNA as part of the Special Latent Cognizant Record Maintenance request.

SYS631 IAFIS (ITN/LPS) shall provide the capability to copy a selected group of records from one SLC file to another as part of the Special Latent Cognizant Record Maintenance request.

SYS632 IAFIS (ITN/LPS) shall provide the capability to allow using the list of FNU(s) or CRN(s) produced by an Ad Hoc Subject Search to identify a set of Criminal Master File or Civil File records to copy to an SLC file as part of the Special Latent Cognizant Record Maintenance request.

SYS633 IAFIS (ITN/LPS) shall provide the capability to request up to the SLC Maximum Number of records be copied from one IAFIS file to an SLC file as part of the Special Latent Cognizant Record Maintenance request.

SYS634 IAFIS (ITN/LPS) shall reject a Special Latent Cognizant Record Maintenance request when the specified SLC File is invalid.

3.6.18.3 Special Latent Cognizant Record Maintenance Request Outputs

SYS635 IAFIS (ITN/LPS) shall provide an appropriate Special Latent Cognizant Record Maintenance response to an Authorized FBI Service Provider via the IAFIS Workstation.

SYS636 IAFIS (ITN/LPS) shall include the reason(s) for rejection of the Special Latent Cognizant Record Maintenance Request.

NGI-347

3.6.19 Computerized Contributor Address (CCA) File Maintenance Request

3.6.19.1 Computerized Contributor Address File Maintenance Request Inputs

SYS637 IAFIS (ITN/DPS) shall accept CCA File Maintenance Requests from Authorized FBI Service Providers via an IAFIS workstation.

3.6.19.2 Computerized Contributor Address File Maintenance Request Processing

SYS638 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to perform an ad hoc CCA File Search Request to III and accept its response as part of the CCA File Maintenance Request.

SYS639 IAFIS (III) shall require the ad hoc CCA File Search Request is to contain an ORI number or state abbreviation code and city (at least the first character).

SYS640 IAFIS (III) shall return all records in the CCA file that match the search parameters specified in the ad hoc CCA File Search Request.

SYS641 IAFIS (ITN/DPS) shall display all records returned the ad hoc CCA File Search Request.

CCA File Modification Requests will be submitted by users to correct erroneous or omitted data, to change the number of response copies, to change addresses, to indicate the response media for non-NCIC responses, or to change the list of agencies that receive copies of responses. CCA file modification information will be entered and verified by ITN/DPS and then forwarded to III for CCA file maintenance.

SYS642 IAFIS (III) shall create a record in the CCA File based on Contributor Address data provided as part of a add contributor CCA File Maintenance Request.

SYS643 IAFIS (III) shall discontinue (retire) a Contributor's Address record based on information provided by an Authorized FBI Service Provider as part of a deactivate contributor CCA File Maintenance Request.

SYS644 IAFIS (III) shall associate a retired Contributor's Address record to another active Contributor Address record based on information provided by an Authorized FBI Service Provider as part of a deactivate contributor CCA File Maintenance Request.

There will be instances where a Contributor's agency or organizational structure changes requiring the consolidation of points of contact with the FBI. The deactivated points of contact (contributor address) will need to be associated with the new or other existing Contributor Address information to facilitate inquiries and reporting of past events.

SYS645 IAFIS (III) shall perform the designated maintenance action on the specified Contributor Address record data as part of the CCA File Maintenance Request.

SYS646 IAFIS (III) shall reject the CCA File Maintenance Request when the maintenance action is unsuccessful.

3.6.19.3 Computerized Contributor Address File Maintenance Request Outputs

NGI-348

SYS647 IAFIS (ITN/DPS) shall provide an appropriate CCA File Maintenance Request response

via the IAFIS Workstation.

SYS648 IAFIS (III) shall include the reason(s) for rejection of the CCA File Maintenance Request.

3.6.20 Computerized Records Sent (CRS) File Maintenance Request

The CRS database, maintained by III, contains records of those agencies that receive copies of responses.

3.6.20.1 Computerized Records Sent File Maintenance Request Inputs

SYS649 IAFIS (ITN/DPS) shall accept Computerized Records Sent (CRS) Modification submissions via IAFIS workstations.

3.6.20.2 Computerized Records Sent File Maintenance Request Processing

SYS650 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to access the Receiving Agency Notification Report (RANR) as part of the CRS File Maintenance request.

SYS651 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to add a record to the CRS file.

SYS652 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to delete a record from the CRS file.

SYS653 IAFIS (III) shall perform the maintenance action designated in a CRS File Maintenance request.

SYS654 IAFIS (III) shall reject the CRS File Maintenance request when the maintenance action is unsuccessful.

3.6.20.3 Computerized Records Sent File Maintenance Request Outputs

SYS655 IAFIS (ITN/DPS) shall provide an appropriate CRS File Maintenance Request response via the IAFIS Workstation.

SYS656 IAFIS (III) shall include the reason(s) for rejection of the CRS File Maintenance Request.

3.6.21 Restore Subject Criminal History Information Request

Restore FNU requests will be submitted by Service Providers to roll back criminal history data, feature data, and image data updates associated with an erroneous consolidation, expungement, FNU deletion, or death notice. A Restore FNU Request may be initiated up to 30 days following the erroneous transactions.

ITN will forward Restore FNU transactions to III, ITN/ISRE, and AFIS to initiate the appropriate restorations of data. The Restore FNU process will be different for records deleted as a result of known deceased ten-print submissions, expungements, deletions, and consolidations.

NGI-349

a. Restore from Deceased. The ITN/DPS Service Provider determines if the record is still restorable (Restore FNU Query and Response). The Service Provider then has the option of initiating a separate Ten-Print search action against the restored FNU to check for activity after the subject was expunged or deleted. If the record is in a restorable state, the Service Provider directs the restoration of the subject (Restore Criminal History Request & File Maintenance Response). Images and features in ITN/ISRE and AFIS are not deleted when the subject is a known deceased.

b. Restore from Expungement or Deletion. The Service Provider follows the steps for Restore from Deceased. Then III initiates the File Maintenance of the other segments, sending the data descriptors for AFIS (File Synchronization Request—III to ITN). ITN restores its image record, and directs AFIS to recreate its features record from the FIMF record (Update Fingerprint Features Request). AFIS sends back the fingerprint classification (Update Fingerprint Features Response) to ITN, who sends it to III (File Maintenance Completion Response).

c. Restore from Consolidation: The Service Provider may reverse the consolidation of several subjects' records temporarily and then consolidate the same records to a previously killed FBI Number. This occurs if the killed FNU has a want or flash posted in III. The Service Provider may also reverse a consolidation and re-establish the subject records permanently.

The Service Provider determines if the record is restorable using a Restore FNU Query. III will return the consolidated record and its restorability status including the subject's record. The Service Provider may print the record if desired. Then the Service Provider may initiate a Restore Criminal History Request to re-establish the previously consolidated records. III will restore the records and initiate the file maintenance of the other segments, i.e., AFIS and ITN/ISRE. File maintenance occurs in the same manner as that for a restoration from an expungement, except ITN directs AFIS to override the quality score of the "kept" FNU and completely update (replace) the record with the calculated features for the images provided by ITN for the "kept" FNU.

An ITN/DPS Service Provider may choose to initiate a FIC in ITN/TPS to verify there is more than one subject. If the restore of the consolidation is to remain permanent, a ITN/DPS Service Provider manually posts any post-consolidation changes to the proper record. If the consolidation request was in error, or if the Service Provider performed the consolidation to consolidate into a different "kept" FNU, the Service Provider consolidates the records with the consolidation process, and manually posts any post-consolidation changes to the record.

3.6.21.1 Restore Subject Criminal History Information Request Inputs

SYS657 IAFIS (ITN/DPS) shall provide the ability for an Authorized FBI Service Provider to query III to determine if a given FNU is restorable via the IAFIS Workstation.

SYS658 IAFIS (ITN/DPS) shall provide the ability for an Authorized FBI Service Provider to submit a Restore Subject Criminal History Requests via IAFIS workstation.

3.6.21.2 Restore Subject Criminal History Information Request Processing

SYS659 IAFIS (III) shall provide a response to a Restore FNU Query indicating whether the given FNU is restorable.

NGI-350

SYS660 IAFIS (III) shall provide, as part of a Restore FNU Query, a list of transactions which

caused updates to a kept FNU, as well as a consolidated record report showing pre-consolidation and post-consolidation record set reports for the kept FNU.

SYS661 IAFIS (ITN/DPS) shall submit the request to restore an FNU to the III Restore FNU service.

SYS662 IAFIS (III) shall process the Restore Subject Criminal History Request according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS663 IAFIS (III) shall restore the criminal history information of the subject contained in a Restore Subject Criminal History Information Request.

SYS664 IAFIS (III/IPS) shall restore all deleted criminal photo images and photo summary data to the previous state when processing a Restore FNU request.

SYS665 IAFIS (III) shall initiate File Synchronization between all segments when processing a restore FNU request.

SYS666 IAFIS (AFIS) shall restore the fingerprint feature data to the previous state when processing a Restore FNU request of an expunged, deleted, or consolidated subject.

SYS667 IAFIS (ITN/ISRE) shall restore the fingerprint image data to the previous state when processing a Restore FNU request of an expunged, deleted, or consolidated subject.

SYS668 IAFIS (III) shall reject a Restore Subject Criminal History Information Request when the store action is unsuccessful.

SYS669 IAFIS (III) shall reject the FNU Restore Query when the specified FNU is invalid.

3.6.21.3 Restore Subject Criminal History Information Request Outputs

SYS670 IAFIS (ITN/DPS) shall provide an appropriate Restore FNU Request response to an Authorized FBI Service Provider via an IAFIS workstation.

3.6.22 NFF Criminal Print Ident Notification

This notification comes from an NFF participant to notify the FBI that a criminal Identification was made at the state level on a given FNU and SID.

3.6.22.1 NFF Criminal Print Ident Notification Inputs

SYS671 IAFIS (III) shall accept an NFF Criminal Print Ident Notification from a III/NFF State via NCIC.

3.6.22.2 NFF Criminal Print Ident Notification Processing

SYS672 IAFIS (III) shall validate FNU and SID included in the NFF Criminal Print Ident Notification prior to generating notifications to Authorized Contributors (e.g., Wanting Agency).

SYS673 IAFIS (III) shall process the NFF Criminal Print Ident Notification according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

3.6.22.3 NFF Criminal Print Ident Notification Outputs

SYS674 IAFIS (III) shall provide an NFF Criminal Print Ident Notification response to a III/NFF State via NCIC.

SYS675 IAFIS (III) shall provide a reject response to an NFF state system when the Criminal Print Ident Notification cannot be processed.

IAFIS (III) will also send the appropriate notifications to III/NFF states that own a portion of the criminal history information in the record being updated. Refer to the *Notification Services System Requirements* section for more information.

3.6.23 Statute Retrieval Requests

The purpose of the IAFIS Statute Retrieval request is to allow an Authorized FBI Service Provider to retrieve statutes for viewing or printing.

3.6.23.1 Statute Retrieval Request Inputs

SYS676 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to submit Statute Retrieval requests in support of AQC using an IAFIS workstation.

SYS677 IAFIS (ITN/TPS) shall require either a State code or a CRI in a Statute Retrieval request.

3.6.23.2 Statute Retrieval Request Processing

SYS678 IAFIS (ITN/TPS) shall retrieve the statute(s) for the State code or CRI indicated in the Statute Retrieval request.

3.6.23.3 Statute Retrieval Request Outputs

SYS679 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to view the statute(s) returned from a Statute Retrieval request on an IAFIS Workstation.

SYS680 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to print the statute(s) returned from a Statute Retrieval request.

3.6.24 Statute Maintenance Request

The purpose of the IAFIS Statute Maintenance request is for an Authorized FBI Service Provider to perform statute maintenance. Once the necessary information is received to initiate a statute maintenance action, an Authorized FBI Service Provider can add, modify or delete a statute and IAFIS will maintain a statute maintenance audit trail for each transaction.

3.6.24.1 Statute Maintenance Request Inputs

SYS681 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to submit Statute Maintenance requests in support of AQC using an IAFIS workstation.

SYS682 IAFIS (ITN/TPS) shall require a designation of file maintenance type (e.g., add, modify, delete) as part of a Statute Maintenance request.

3.6.24.2 Statute Maintenance Request Processing

SYS683 IAFIS (ITN/TPS) shall perform the appropriate file maintenance for the statute as indicated in the Statute Maintenance request.

3.6.24.3 Statute Maintenance Request Outputs

SYS684 IAFIS (ITN/TPS) shall provide the appropriate response to an Authorized FBI Service Provider for a Statute Maintenance request.

3.6.25 Shared Data Direct Enrollment

The following section contains the functional requirements that support the enrollment of records into the iDSM. The process of enrolling implies an addition to the iDSM. The iDSM is comprised of the IAFIS Shared Want Files which contain IAFIS records and the DHS Shared Watch Files which contain IDENT records.

3.6.25.1 Inputs

SYS2181 IAFIS (iDSM) shall accept shared data enrollment requests (e.g., want, warrants) from III on a periodic basis.

Shared Data enrollment requests consist of IAFIS submissions that indicate a want or warrant posted in the Subject Criminal History file for the submitted images. These images for the identified IAFIS Shared Data FNUs are pulled into iDSM from the ITN DISR.

SYS2182 IAFIS (iDSM) shall require an FNU as part of a shared data enrollment request from III.

SYS2183 IAFIS (iDSM) shall retrieve for the designated Shared Data FNUs the corresponding images from ITN.

SYS2184 IAFIS (iDSM) shall accept 14 ANSI/NIST Type 4 image records from ITN as part of a shared data enrollment request.

SYS2185 IAFIS (iDSM) shall compress all images enrolled as part of a shared data enrollment request from ITN using Wavelet Scalar Quantization (WSQ) at a ratio 15:1.

SYS2186 IAFIS (iDSM) shall require the subject's gender, name and date of birth (DOB) from III as part of a shared data enrollment request.

SYS2187 IAFIS (iDSM) shall accept shared data enrollment requests from IDENT via the CJIS WAN.

Enrollment requests from IDENT will be stored in the DHS Shared Watch file.

SYS2188 IAFIS (iDSM) shall accept two ANSI/NIST Type 4 image records from IDENT as part of a shared data enrollment request.

SYS2189 IAFIS (iDSM) shall accept 14 ANSI/NIST Type 4 image records from IDENT as part of a shared data enrollment request.

SYS2190 IAFIS (iDSM) shall be able to read the latest version of fingerprint images available for all individuals provided by IDENT as part of a shared data enrollment request.

SYS2191 IAFIS (iDSM) shall de-compress all fingerprint images in accordance using Wavelet Scalar Quantization (WSQ) at ratio 15:1 as part of a shared data enrollment request from IDENT.

3.6.25.2 Processing

SYS2192 IAFIS (iDSM) shall extract fingerprint features from the fingerprint images provided by IDENT as part of a shared data enrollment request.

SYS2193 IAFIS (iDSM) shall store in the Shared Watch File the extracted fingerprint features received as part of a shared data enrollment request from IDENT.

SYS2194 IAFIS (iDSM) shall remove fingerprint images received as part of a shared data enrollment request from IDENT within 24 hours following a successful features extraction.

SYS2195 IAFIS (iDSM) shall perform a Ten-Print Fingerprint Investigative Image Search (TPIS) as a result of a shared data enrollment request from IDENT.

SYS2196 IAFIS (iDSM) shall generate a list of candidates as the result of a Ten-Print Investigative Image Search initiated by a shared data enrollment request from IDENT.

SYS2197 IAFIS (iDSM) shall determine a "match score" for each candidate resulting from a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT.

SYS2198 IAFIS (iDSM) shall determine a positive identification decision for each candidate that has a match score above the high confidence threshold as a result of a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT.

SYS2199 IAFIS (iDSM) shall require an Authorized FBI Service Provider to perform a manual image comparison for each candidate resulting from a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT that is below the high confidence threshold.

SYS2200 IAFIS (iDSM) shall require a second Authorized FBI Service Provider to perform a manual image comparison to confirm a positive identification for each candidate resulting from a Ten-Print Fingerprint Investigative Image Search initiated by a shared data enrollment request from IDENT that is below the low confidence threshold.

SYS2201 IAFIS (iDSM) shall store all candidates and their correlating EID resulting in a positive identification as a result of a Ten-Print Investigative Image Search initiated by a shared data enrollment request from IDENT.

NGI-354
iDSM will maintain the FNUs and DHS unique id (EIDs) of all idented Shared Watch List Candidates

that are in IAFIS.

3.6.25.3 Output

SYS2202 IAFIS (iDSM) shall reject a shared data enrollment request that fails to include a valid ORI.

SYS2203 IAFIS (iDSM) shall generate an Error Message to IDENT resulting from a failed shared data enrollment request from IDENT.

3.6.26 Shared Data Maintenance

Maintenance messages from IAFIS include removals and demotions. A demotion is a canceled Want in IAFIS that may be maintained in IDENT if a previous encounter has occurred. Maintenance messages from IDENT include only deletions.

3.6.26.1 Inputs

SYS2204 IAFIS (iDSM) shall accept a shared data removal request from III.

SYS2205 IAFIS (iDSM) shall accept a shared data demotion request from III.

SYS2206 IAFIS (iDSM) shall accept a shared data removal requests from IDENT.

SYS2207 IAFIS (iDSM) shall be able to read the latest version of fingerprint images available for all individuals provided as part of a Shared Data Maintenance request.

3.6.26.2 Processing

SYS2208 IAFIS (iDSM) shall remove all biometric and biographic information for an individual identified in a shared data removal request from III.

SYS2209 IAFIS (iDSM) shall remove all biometric and biographic information for individuals identified in a shared data demotion request from III.

SYS2210 IAFIS (iDSM) shall remove all biometric and biographic information for individuals identified in a shared data removal request from IDENT.

SYS2211 IAFIS (iDSM) shall identify the DHS unique identifier for any individuals for whom the DHS received an order to remove or demote.

SYS2212 IAFIS (iDSM) shall be able to match the DHS unique identifier and the corresponding images for each individual provided by IDENT.

3.6.26.3 Outputs

SYS2213 IAFIS (iDSM) shall generate an Error Message resulting from a failed shared data maintenance request.

SYS2214 IAFIS (iDSM) shall generate an Error Message to IDENT resulting from a failed IDENT shared data maintenance request.

NGI-355

3.7 Internal Processing Requirements

The following section contains the functional requirements relating to the internal IAFIS processes which support the IAFIS user services. These requirements provide the automated functions necessary to provide end-to-end transaction processing.

3.7.1 Workflow Management

3.7.1.1 EFCON Workflow Management

SYS685 IAFIS (EFCON) shall provide the capability to create transaction queues based on system transaction types and special qualifications.

SYS686 IAFIS (EFCON) shall provide the capability to queue CJIS WAN transactions.

EFCON queuing will occur when the incoming rate of transactions exceeds the throttle controlling injection into IAFIS or IAFIS is not operating. In addition, EFCON will queue transactions that are of a type or is from a contributor that is always queued.

SYS687 IAFIS (EFCON) shall provide the total queue capacity to queue up to three days of CJIS WAN transactions for transmittal into IAFIS.

SYS688 IAFIS (EFCON) shall provide the hourly queue capacity to hold three times the peak hour number of system transactions.

SYS689 EFCON shall send queued system transactions to the ITN Workflow manager when the requested processing capability is available.

SYS690 EFCON shall hold all submitted transactions until the ITN Workflow manager is ready to process the requests.

SYS691 IAFIS (EFCON) shall provide an indication to the Authorized Contributor when the system is not able to accept additional transactions.

SYS692 EFCON shall provide transactions of the same priority to the ITN Workflow manager in the same order in which they are received (first in, first out).

SYS693 IAFIS (EFCON) shall provide queued system transactions to the system in accordance with the established queue priority rules.

SYS694 IAFIS (EFCON) shall automatically resume transmission of a queued message which was pre-empted whenever the communication channel is available and no higher priority traffic is waiting.

When communication between EFCON and IAFIS is interrupted, submissions are queued. When communication is restored, queued submissions are sent to IAFIS based on priority, but limited in number by an established threshold minus the measured rate of incoming non-queued submissions.

SYS695 IAFIS (EFCON) shall support precedence and pre-emption prioritization among external communications traffic and queued submissions.

SYS696 IAFIS (EFCON) shall support precedence priority, including queued submissions, by selecting a higher priority message over a lower priority message for transmission.

Some submissions with a lower priority may be queued rather than sent to IAFIS, otherwise messages are sent to IAFIS in FIFO order, subject to threshold limitations.

SYS697 IAFIS (EFCON) shall support pre-emption priority, including queued submissions, by suspending a lower priority message and sending a higher priority message, even if the higher priority message arrives after the lower priority message has started transmission.

The transmission of a message is never suspended once it has started. For a queued message, the decision to transmit is made taking into account the priority of all other queued messages. For an incoming external submission, the decision to either transmit or queue occurs independently of the status of any currently transmitting queued message. Transmission of a message in both cases will only occur when the current transmissions rate of external submission does not exceed the threshold for injections into IAFIS.

SYS698 IAFIS (EFCON) shall contain a metering system that will monitor and control the hourly transaction flow rate into IAFIS.

SYS699 IAFIS (EFCON) shall provide the capability to establish and modify the flow rate as needed.

SYS700 IAFIS (EFCON) shall provide an automated method to promptly recover any transaction received over the last several months and provide it to IAFIS for processing.

SYS701 IAFIS (EFCON) shall promptly retrieve and re-send a response from the online storage, at the request of the contributing agency.

Whenever a contributing agency's system is off-line, its responses will be stored in a queue until its system is back on-line.

SYS702 IAFIS (EFCON) shall provide the capability to queue undeliverable outgoing responses.

SYS703 IAFIS (EFCON) shall send or resend queued responses when a contributing agency is back on-line.

SYS704 IAFIS (EFCON) shall stop accepting additional outgoing responses when the queue is full, and notify the sending segment of the message refusal.

SYS705 IAFIS (EFCON) shall attempt to deliver queued responses when possible.

SYS706 IAFIS (EFCON) shall have queue capacity to hold three times the peak hour number of responses.

3.7.1.2 IAFIS Workflow Management

SYS707 IAFIS shall provide system transaction access control.

SYS708 IAFIS shall ensure that all the required processing of each segment and inter-segment transactions have been completed.

SYS709 IAFIS shall manage the processes for each transaction based on the transaction type and the outcome of each processing step for each segment.

SYS710 IAFIS shall provide the capability to queue system transactions that cannot be forwarded to the appropriate processing segment, element, sub-element, or external interface.

NGI-357

SYS711 IAFIS shall queue all complying submissions for processing.

SYS712 IAFIS shall determine the appropriate processing flow for each type of IAFIS input, based upon the system transaction type and outcome from of each processing step.

A segment owner is designated for each IAFIS transaction type. In its ownership capacity, the segment is responsible for input validation, rejecting unsatisfactory requests, managing the workflow processes, ensuring system transactions are properly processed, determining when processing for a system transaction is completed, and maintaining the transaction history.

SYS713 IAFIS shall manage system transaction ownership.

SYS714 IAFIS shall provide transit queues for each manual function in its work group profiles.

SYS715 IAFIS shall manage each Automated Function (e.g., ITN/ISRE, ICR, III) workload.

SYS716 IAFIS shall process inter-segment and intra-segment Automated Function transactions and return responses within response time requirements.

SYS717 IAFIS (ITN/TPS) shall support submission deadlines.

A submission-level deadline is used to help detect when submissions have not moved through ITN quickly enough to meet the response time requirements.

SYS718 IAFIS (ITN/TPS) shall support function-level deadlines.

A function-level deadline is used to detect when a Service Provider has not started processing a submission soon enough or to detect when a submission has been sitting in a queue too long.

SYS719 IAFIS (ITN/TPS) shall provide a queue to track work sent to an Automated Function.

SYS720 IAFIS (ITN/TPS) shall provide a collection of queues corresponding to each function in the work group profile of the Work Group Transit Queue Structure.

SYS721 IAFIS (ITN/TPS) shall provide a route to the next required processing function for each system, intra-segment, and inter-segment transaction requiring further processing.

SYS722 IAFIS (ITN/TPS) shall manage the workload and workflow for all manually supported functions.

SYS723 IAFIS (ITN/TPS) shall support the removal and redistribution of inter-segment and intra-segment transactions waiting for processing.

SYS724 IAFIS (AFIS) shall provide the capability to queue segment data or input/output data for resubmission in the event of internal component unavailability or system unavailability.

SYS725 IAFIS (AFIS) shall provide a queuing capability able to accommodate outages of up to 24 hours.

SYS726 IAFIS (ITN/TPS) shall forward the submission and error message(s) for those logic errors that may be repairable to an Authorized FBI Service Provider as part of the LER function.

SYS727 IAFIS shall provide the capability to queue inter-segment transactions that cannot be forwarded to the appropriate processing segment, element, sub-element, or external interface.

SYS728 IAFIS shall provide the capability to queue intra-segment transactions that cannot be forwarded to the appropriate processing element or sub-element.

SYS729 IAFIS (ITN) shall provide application level acknowledgments for the processing of system, intra-segment, and inter-segment transactions.

NGI-358

SYS730 IAFIS (ITN) shall determine if intra-segment or inter-segment transaction results require special processing. (Service Desk, Special Stops, and Wants review.)

SYS731 IAFIS (ITN) shall suspend processing of the segment transaction and associated system transaction during special processing review until reviewer releases transaction to continue normal processing.

SYS732 IAFIS (ITN) shall route the segment transaction requiring a review to the reviewers queue so the transaction can be reviewed and released.

SYS733 IAFIS (ITN) shall notify the appropriate Authorized FBI Service Provider when routing the transaction to special processing review.

SYS734 IAFIS (ITN) shall provide the ability to coordinate synchronized updates between IAFIS segments.

ITN will control the workflow management for all file maintenance actions (i.e., fan-out, rendezvous).

SYS735 IAFIS (ITN) shall schedule system transaction inputs to ensure that response times are maintained for each type of submission.

SYS736 IAFIS (ITN) shall have a scheduling precedence table that will be used to determine which submissions have precedence in scheduling conflicts.

SYS737 IAFIS (ITN) shall rank submission types and response time requirements in accordance with the precedence table. (Note: this ranking is via response due time.)

SYS738 IAFIS (ITN) shall compute the processing sequence using the precedence table to determine which submissions receive resources when conflicts occur.

SYS739 IAFIS (ITN) shall assign each submission to a queue for processing.

SYS740 IAFIS (ITN) shall assign submissions requiring automated processing to an automated processor queue.

SYS741 IAFIS (ITN) shall assign submissions requiring manual intervention to the appropriate functional work group queues authorized to process the submission.

SYS742 IAFIS shall provide the capability to queue incoming system and inter-segment transactions.

SYS743 IAFIS shall provide the ability to cease accepting new system and inter-segment transactions until the outage has been repaired.

SYS744 IAFIS shall provide the capability to continue to process those system, inter-segment, or intra-segment transactions that are unaffected by the outage.

SYS745 IAFIS shall provide the capability to queue outgoing system and inter-segment transactions to the affected IAFIS capability area until the outage has been repaired.

SYS746 IAFIS (ITN) shall initially schedule system transactions for delivery to the processing segment, element, or sub-element based on each system transaction's arrival time and priority.

3.7.1.3 Identification Workflow

SYS747 IAFIS (ITN) shall route submissions that require verification processing to another individual to perform the manual processing verification functions.

SYS748 IAFIS (ITN) shall route transactions to authorized FBI Service Providers assigned to work groups that are authorized to perform the function.

SYS749 IAFIS (ITN) shall ensure that an authorized FBI Service Provider does not verify their own work.

SYS750 IAFIS (ITN) shall provide the next transaction in the queue for which the work group member has not performed work on the transaction.

SYS751 IAFIS (ITN) shall send the next transaction to the workstation in advance so that it is immediately available for processing when the authorized FBI Service Provider is ready to process the transaction.

The process of sending the next task to the workstation in advance of being worked is known as 'pre-staging' the work.

SYS752 IAFIS (ITN) shall route transactions from inactive work group queues to active work group queues.

3.7.1.3.1 Support Transaction Forwarding Processing

The Ten-Print Transaction Forwarding process can be performed on the QC, FSC, FIC, and LER functions.

SYS753 IAFIS (ITN/TPS) shall support a four level hierarchical skill level structure in support of Ten-Print processing.

The four levels are: Level 1—Service Provider; Level 2—Experienced Service Provider/team leader; Level 3—Area Supervisor; Level 4—Operations Manager.

SYS754 IAFIS (ITN/TPS) shall provide the capability to forward according to baseline forwarding rules outlined in Table 3.7.1-1.

Table 3.7.1-1 Baseline Forwarding Rules

Function	Service Provider Level	Forward Authorization	Forward Destination
All Functions	Level 1	Yes	Level 2
	Level 2	Yes	Level 2/3
	Level 3	Yes	Level 3/4
	Level 4	Yes	Level 3/4

During a shift change, a transaction that was forwarded to a Level 3 or Level 4 Service Provider and was not processed, will be forwarded to Level 3 or Level 4 Service Provider on the next shift. Based on these rules, transactions are forwarded to Service Providers of the appropriate Level for a function and not to specific Service Providers. The exception to this rule is that a Level 4 Service Provider can forward to a specific Level 3 or Level 4 Service Provider.

3.7.1.3.2 Support QA Processing

SYS755 IAFIS (ITN/TPS) shall queue system transactions at a volume that will ensure that all

NGI-360

QA Service Providers are continually supplied with transactions.

SYS756 IAFIS (ITN/TPS) shall provide the capability to adjust the sampling rate to the system transaction volume to prevent queuing up too many or too few transactions.

The process of giving a sampling of system transactions is known is the 'QA Drain'. This process looks at the amount work in the QA queue, the response due time for that work, the number of Service Providers performing the QA function, and the rate at which the work is being completed. These amounts are used to determine how much work should remain the QA queue and moves the remaining work on to the next function so that response times are met.

SYS757 IAFIS (ITN/TPS) shall forward the QA system transaction to the evaluation unit if the correction will have an impact on the results of the original search.

SYS758 IAFIS (ITN/TPS) shall return the QA system transaction to the original step in the workflow if no correction is needed, or if the correction has no impact on the original search results.

3.7.1.3.3 Support PPR Processing

SYS759 IAFIS (ITN/TPS) shall retain all forwarded transactions including images, text, and the reasons for forwarding along with the associated resolutions.

SYS760 IAFIS (ITN/TPS) shall provide the capability for authorized FBI Service Providers to define the number of days that forwarded transactions are retained.

SYS761 IAFIS (ITN/TPS) shall retain two days worth of forwarded transactions as a default, with this being an adjustable parameter.

SYS762 IAFIS (ITN/TPS) shall automatically delete forwarded transactions that are retained beyond the defined forwarded review period.

SYS763 IAFIS (ITN/TPS) shall retain all rejected transactions including images, text, and the reason for the rejection.

SYS764 IAFIS (ITN/TPS) shall allow a rejection review after the transaction has completed processing and will not impact the time allocated to processing the transaction.

SYS765 IAFIS (ITN/TPS) shall provide the capability for authorized FBI Service Providers to define the number of days that rejected transactions are to be retained.

SYS766 IAFIS (ITN/TPS) shall retain two days worth of rejected transactions as a default, with this being an adjustable parameter.

SYS767 IAFIS (ITN/TPS) shall automatically delete rejected transactions that are retained beyond the defined rejection review period.

3.7.1.4 Investigation Workflow

SYS768 IAFIS (AFIS) shall have a capacity to maintain five days of pending latent searches against the CMF repository.

SYS769 IAFIS (AFIS) shall select and process a group of latent searches from the entire list of pending latent searches.

SYS770 IAFIS (AFIS) shall provide the capability to maintain Latent Search Allocation business rules for states, federal organizations, and the FBI's Latent Fingerprint Processing Section

(LFPS).

SYS771 IAFIS (AFIS) shall select and process latent searches from the pending search list according to the Latent Search Allocation business rules.

SYS772 IAFIS (AFIS) shall process latent searches in First In, First Out (FIFO) order, within a given priority.

SYS773 IAFIS (AFIS) shall provide the capability to select and process the highest priority searches from those remaining in FIFO order if additional capacity is available during any period.

SYS774 IAFIS (AFIS) shall reject latent searches from users and Latent Specialists that exceed their organization's latent search allocation.

SYS775 IAFIS (AFIS) shall process all pending searches for a given organization in priority order.

Higher priority searches will be performed before lower priority searches independent of the date and time when they were submitted.

SYS776 IAFIS (AFIS) shall provide the capability to create and manage queues for latent fingerprint searching.

3.7.1.5 Workflow Administration

SYS777 IAFIS (ITN) shall support operator definition of the sequence of functions in the workflow process (workflow routing rules).

SYS778 IAFIS (ITN) shall provide the capability for a system administrator to enter, modify, and delete workflow routing rules.

SYS779 IAFIS (ITN) shall support workflow entry and modifications through the use of a graphical interface providing the capability of reviewing changes in a pictorial representation for each workflow.

SYS780 IAFIS (ITN) shall provide the capability for the system administrator to specify each input type and format for each workflow.

An operator may map civil hardcopy submissions to a particular workflow and criminal hardcopy submissions to another.

SYS781 IAFIS (ITN) shall require that all routing rules are unique.

SYS782 IAFIS (ITN) shall provide tools that test workflow modifications to show improvement in system efficiency.

SYS783 IAFIS (ITN) shall provide the capability for system administrator to monitor all workflows.

SYS784 IAFIS (ITN) shall support a configurable rule list that specifies the actions to take for each submission deadline.

SYS785 IAFIS (ITN) shall support a configurable rule list that specifies the actions to take for each function deadline.

NGI-362

These lists can be adjusted by an Authorized FBI Service Provider. No e-mail messages are sent when deadlines occur. The workflow manager will not automatically forward submissions to the Team Leader when deadlines occur.

SYS786 IAFIS (ITN) shall provide the capability for a system administrator to set thresholds on queue sizes.

When the screen is refreshed, if the threshold for a queue is reached, the Authorized Service Provider is alerted. (Note: The queues that are monitored by the Service Provider are bolded so the eye finds them readily.)

SYS787 IAFIS (ITN) shall indicate when a queue exceeds the monitoring threshold established by an Authorized FBI Service Provider.

SYS788 IAFIS (ITN) shall provide the capability for a system administrator to modify the priority of the transaction via the Workflow Management Tool.

SYS789 IAFIS (ITN) shall provide the capability for an authorized administrator to modify the scheduling precedence table by adding, deleting, and modifying entries.

SYS790 IAFIS (AFIS) shall provide a priority processing scheme with at least 12 levels of priority designation for the search function.

3.7.2 Compression/Decompression

SYS791 IAFIS shall store fingerprint images in a compressed format.

SYS792 IAFIS shall transmit fingerprint images in a compressed format.

SYS793 IAFIS shall provide the capability to compress fingerprint images in accordance with the Electronic Fingerprint Transmission Specification (EFTS).

SYS794 IAFIS shall provide the capability to decompress fingerprint images in accordance with the EFTS.

SYS795 IAFIS shall provide decompression functionality to support AFIS Feature Extraction function.

SYS796 IAFIS (ITN/TPS) shall support the decompression of images for display.

SYS797 IAFIS (ITN/TPS) shall support the decompression of images for printing.

SYS798 IAFIS (ITN) shall provide the capability to compress scanned fingerprint images prior to storage in ISRE.

3.7.3 Automated Fingerprint Sequence Check (ASC) Function

SYS799 IAFIS (AFIS) shall maintain an ASC Pass Flag to indicate pass or fail.

SYS800 IAFIS (AFIS) shall perform ASC when the Perform ASC flag is set to 'Y'.

SYS801 IAFIS (AFIS) shall compare a submission's plain impressions to the rolled impressions and develop an ASC score based on the number of matching plain finger and rolled impressions.

SYS802 IAFIS (AFIS) shall consider the submission in sequence if one or both of the little finger plain impressions are missing and the rest of the impressions are in sequence.

SYS803 IAFIS (AFIS) shall set the ASC Pass Flag to a passing value if the minimum ASC score is met on at least nine fingers.

SYS804 IAFIS (AFIS) shall set the ASC Pass Flag to a non-passing value if the minimum ASC score is not met on any two fingers.

SYS805 IAFIS (AFIS) shall set the ASC Pass Flag to a non-passing value if the minimum number of rolled fingers is not present.

SYS806 IAFIS (AFIS) shall set the ASC Pass Flag to a non-passing value if the minimum number of fingers in the plain impression does not exist.

3.7.4 III/Verify Function

Ten-Print fingerprint submissions that contain an FBI Number as part of the data set are referred to as "quoted FNU" submissions. Those submissions along with the submissions that receive a candidate during the Subject Search are forwarded to the III/Verify function to ensure that the images in the submission closely match the "quoted FNU" or the Subject Search candidates.

SYS807 IAFIS (AFIS) shall retrieve the features for each candidate provided to the III/Verify function.

SYS808 IAFIS (AFIS) shall compare the fingerprint features of the incoming fingerprint submission to the retrieved fingerprint features of each candidate provided to III/Verify function.

SYS809 IAFIS (AFIS) shall determine a "match score" for each III/Verify candidate.

SYS810 IAFIS (AFIS) shall indicate a non-identification decision for each III/Verify candidate that has a match score below the minimum III/Verify threshold.

SYS811 IAFIS (AFIS) shall forward the fingerprint submission features to the fingerprint features search when the III/Verify fingerprint match scores of all III candidates do not meet the defined match score threshold.

SYS812 AFIS shall return to ITN/TPS the III/Verify candidates that have a match score above the minimum threshold.

3.7.5 Feature Search

SYS813 IAFIS (AFIS) shall extract fingerprint features from the fingerprint images when no features are provided in the feature search.

The fingerprint features extracted include information such as pattern class, ridge counts, minutiae, core/delta locations, and quality metrics.

SYS814 IAFIS (AFIS) shall assign a confidence rating to each classification indicating the reliability of the classification as part of any feature extraction.

SYS815 IAFIS (AFIS) shall assign reference fingerprint classifications when there is uncertainty in classification as part of any feature extraction.

SYS816 IAFIS (AFIS) shall perform a feature search of the specified repository using fingerprint features and optional search parameters.

NGI-364

AFIS will use optional search parameters to limit the file penetration for a Latent Fingerprint Feature Search. Optional search parameters consist of the following data elements for latent searches against the CMF: Gender; Race; Height (with range); Weight (with range); Pattern Class and Ridge Count (with Reference Class if Pattern Classification is used and ranges if subordinate classification is used); Finger Number (including a range); Age (with range); Hair Color; Eye Color; Scars, Marks, and Tattoos; Place of Birth.

SYS817 IAFIS (AFIS) shall return up to the maximum number of candidates in response to a feature Search request.

SYS818 IAFIS (AFIS) shall include, on the feature search candidate list, the candidates with match scores above the applicable threshold.

SYS819 IAFIS (AFIS) shall include the identification number (FNU, CRN, SLCN), match score, and confidence level for each ten-print search candidate.

SYS820 IAFIS (AFIS) shall include the identification number (FNU, CRN, SLCN), match score, and finger number matched for each latent search candidate.

The SLCN is the unique identifier of the Special Latent Cognizant File.

3.7.6 Image Storage and Retrieval Element (ISRE)

The Ten-Print Certification File (TPCF), Criminal Ten-Print Fingerprint Image Master File (FIMF), Civil On-Line Image File, Unsolved Latent Image File (ULF), and Special Cognizant Latent File (SLC) repositories are part of the ITN/ISRE.

SYS821 IAFIS (ITN/ISRE) shall retrieve fingerprint images from the designated repository in response to a fingerprint image request.

3.7.6.1 FIMF Repository

SYS822 IAFIS (ITN/ISRE) shall provide the capability to add digitized composite criminal ten-print fingerprint images (FIMF).

SYS823 IAFIS (ITN/ISRE) shall provide the capability to replace digitized composite criminal ten-print fingerprint images (FIMF).

A FIMF image replacement may be a full or partial replacement, but will always result in a new image being created with an update to the index to point to the newly created image. The existing image is not physically deleted and can be retrieved by using the ICN which created the image.

SYS824 IAFIS (ITN/ISRE) shall provide the capability to delete digitized composite criminal ten-print fingerprint images (FIMF).

SYS825 IAFIS (ITN/ISRE) shall retrieve composite images from the FIMF using the FNU.

SYS826 IAFIS (ITN/ISRE) shall have the capability to access images from the FIMF using the ICN that was used to add the fingerprint image.

3.7.6.2 Civil On-line Repository

SYS827 IAFIS (ITN/ISRE) shall provide the capability to add digitized civil ten-print fingerprint

images.

SYS828 IAFIS (ITN/ISRE) shall retrieve civil ten-print images from the Civil Ten-Print On-Line File using the Civil Record Number (CRN).

3.7.6.3 ULF Repository

SYS829 IAFIS (ITN/ISRE) shall provide the capability to create unsolved latent fingerprint images in the ULF.

SYS830 IAFIS (ITN/ISRE) shall provide the capability to delete unsolved latent fingerprint images from the ULF.

SYS831 IAFIS (ITN/ISRE) shall provide the capability to retrieve unsolved latent fingerprint images in the ULF by the SCNA index number.

3.7.6.4 SLC Repository

The SLC Files consist of fingerprint images from the different ITN/ISRE repositories and fingerprint images submitted by authorized agencies. The features for these SLC files are contained in AFIS. However, an SLC File may be a separate collection of image records or a logical grouping of records in other ITN/ISRE repositories, or some combination of both.

SYS832 IAFIS (ITN/ISRE) shall provide the capability to create images in an SLC.

SYS833 IAFIS (ITN/ISRE) shall provide the capability to delete images from an SLC.

SYS834 IAFIS (ITN/ISRE) shall provide the capability to retrieve images from an SLC using the FBI Number or other unique identifier.

SYS835 IAFIS (ITN/ISRE) shall allow Authorized FBI Service Providers to access only those SLC files to which they have been granted access.

Latent Specialists will be granted privileges to add, delete, update, or retrieve records in those files that are created by authorized specialists at their request.

SYS836 IAFIS (ITN/ISRE) shall notify ITN/LPS when Criminal Master File records are deleted as part of an expungement or consolidation and the deleted records correspond to records stored in an SLC.

SYS837 IAFIS (ITN/ISRE) shall delete record copies from any SLC when the same record is deleted from FIMF.

3.7.6.5 Latent Image File (LIF)

The images in the LIF, containing photos of complete and partial fingerprint and palm print images, will be used during criminal investigations performed by the FBI Latent Fingerprint Processing Section.

SYS838 IAFIS (ITN/ISRE) shall provide the capability to create latent images in the LIF.

SYS839 IAFIS (ITN/ISRE) shall provide the capability to delete latent images from the LIF.

SYS840 IAFIS (ITN/ISRE) shall provide the capability to retrieve latent images in the LIF by a combination of case number, case extension, and image designation.

3.7.6.6 Major Case Print File (MCP)

A Major Case print contains the fingerprint and all the friction ridge detail present on the palmar surfaces of the hands and the inner surfaces of the fingers.

SYS841 IAFIS (ITN/ISRE) shall provide the capability to create images in the MCP.

SYS842 IAFIS (ITN/ISRE) shall provide the capability to delete images from the MCP.

SYS843 IAFIS (ITN/ISRE) shall provide the capability to retrieve images in the MCP using the FBI Number or other unique identifier.

3.7.6.7 Restore Image Request

SYS844 IAFIS (ITN/ISRE) shall provide the capability to restore FIMF image records to previous state using the ICN.

The restore activity includes returning the composite fingerprint using the ICN associated with the add request. This restore activity is associated with a full expungement, deletion, and consolidation.

3.7.6.8 Respond to Image Request

SYS845 IAFIS (ITN/ISRE) shall write the retrieved image into the indicated folder in the appropriate repository (e.g., TEFF,LEFF).

SYS846 IAFIS (ITN/ISRE) shall return a status message for all request types to the calling function as defined in ITN Software Design Document.

The status message will include an accept message or a reason why the image retrieval or maintenance request was not completed.

3.7.6.9 Delete Image Data

Expungements and 'killed' consolidation records are defined as a type of deletion. Both of these requests will be performed using delete operations.

SYS847 IAFIS (ITN/ISRE) shall mark deleted record(s) in the indices to ensure that the record cannot be accessed under normal operational conditions.

3.7.6.10 Biometric Data Storage

EFCON has the capability to receive, store, and track biometric data submitted by contributors in the form of photo input (Type 10), flat fingerprint data (Type 14), palm print data (Type 15), or iris data (Type 17) records as part of a Ten-Print Fingerprint Identification Search request. All submissions, including those with biometric data, are written, without modification, to a file system when received by EFCON. Certain EFCON tables contain columns representing the four biometric record types mentioned above. These columns are updated with a count of the number of records of each biometric type for each submission.

Only Type 10 and Type 14 records undergo any processing by EFCON. Type 10 records are passed on to ITN in submissions with certain Photo related TOTs. EFCON converts Type 14

records to Type 4 records for submissions with TOTs that require Type 4 images. Otherwise, biometric records are removed from the submission prior to passing it to ITN.

SYS848 IAFIS (EFCON) shall provide the capability to store photo data.

SYS849 IAFIS (EFCON) shall provide the capability to store flat fingerprint images.

SYS850 IAFIS (EFCON) shall provide the capability to store palm print images.

SYS851 IAFIS (EFCON) shall provide the capability to store iris data.

3.7.7 Post Latent Process

IAFIS periodically performs a correlation process looking for all latent search results that contain the same candidate(s). IAFIS then reports the correlation back to the Latent Service Provider.

SYS852 IAFIS (AFIS) shall periodically compare stored search results for each individual case to determine if the same candidate FNU or CRN appears in more than one candidate list.

SYS853 IAFIS (ITN/LPS) shall notify the Authorized FBI Service Provider when a correlation between candidate lists within an individual case is determined to exist.

SYS854 IAFIS (AFIS) shall record the correlation of same FNU/CRN on two different Candidate Lists into a stored "correlation list."

SYS855 IAFIS (AFIS) shall have a configurable time interval in which to initiate the "correlation process."

SYS856 IAFIS (AFIS) shall maintain the "correlation list" for a configurable time period.

SYS857 IAFIS (AFIS) shall provide additional candidates as part of a Latent Fingerprint Search request from an independent correlation of candidate lists from prior latent searches of the CMF.

SYS858 IAFIS (ITN/LPS) shall create the Post Latent Processing (PLP) search entry in the Latent Electronic File Folder (LEFF) for the first correlation data of the LFS Submission Log entry as defined by a unique Latent Case Number (LCN).

SYS859 IAFIS (ITN/LPS) shall update the PLP search entry in the LEFF for the second or more correlation data of the LFS Submission Log entry as defined by a unique ICN.

3.7.8 Response Generation

SYS860 IAFIS shall provide responses to user requests.

SYS861 IAFIS (III) shall generate response messages in accordance with the IAFIS ICD, the III/NFF Operational and Technical Manual, and the MRD Disposition Specification.

SYS862 IAFIS shall generate responses for submissions (when a response is required) in accordance with the IAFIS ICD and the IAFIS Message Definition Database (MDD).

SYS863 IAFIS shall generate responses for searches when a response is required in accordance with the IAFIS ICD and the IAFIS Message Definition Database (MDD).

SYS864 IAFIS shall generate responses for service requests when a response is required in accordance with the IAFIS ICD and the IAFIS Message Definition Database (MDD).

NGI-368

SYS865 ITN shall compile response information for document submissions and provide the compiled response information to III for final preparation, formatting and transmission.

SYS866 IAFIS (III) shall validate all incoming response messages to determine if they are ready for response or require operator intervention or error handling.

SYS867 IAFIS (III) shall refer exceptions and errors to an authorized III operator for review and corrective action.

SYS868 IAFIS (III) shall add new information to the Computerized Records Sent File during response generation.

3.7.8.1 Subject Criminal History Rap Sheet (IDRR)

SYS869 IAFIS (III) shall provide an FNU as part of a Subject Criminal History Rap Sheet.

SYS870 IAFIS (III) shall include biographic identifiers (e.g., Name, AKA, DOB) on the Subject Criminal History Rap Sheet.

SYS871 IAFIS (III) shall include arrest event information (e.g., Date of Arrest, arresting agency ORI) on the Subject Criminal History Rap Sheet.

SYS872 IAFIS (III) shall include civil event information (e.g., date fingerprinted, submitting ORI) on the Subject Criminal History Rap Sheet.

SYS873 IAFIS (III) shall include want information on the Subject Criminal History Rap Sheet.

SYS874 IAFIS (III) shall provide active Flash information as part of the Subject Criminal History Rap Sheet.

SYS875 IAFIS (III) shall include SOR information on the Subject Criminal History Rap Sheet.

The inclusion of arrest, civil, want and SOR information on the Subject Criminal History Rap Sheet is subject to the response generation rules. For example, civil cycles and returned arrest prints may not appear on a Subject Criminal History Rap Sheet sent to an external agency but will appear on an internal Subject Criminal History Rap Sheet.

SYS876 IAFIS (III) shall include criminal photo summary information in the Subject Criminal History Rap Sheet.

SYS877 IAFIS (III) shall provide an indication of a photo on file as part of the Subject Criminal History Rap Sheet.

SYS878 IAFIS (III) shall apply response generation rules when generating and disseminating the Subject Criminal History Rap Sheet.

SYS879 IAFIS (III) shall include a "sealed data" flag with criminal history data retrieved by III for display on an ITN workstation screen.

SYS880 IAFIS (III) shall include criminal history information from NFF state systems in the Subject Criminal History Rap Sheet in support of the NFF program.

3.7.8.2 Response Generation Rules

SYS881 IAFIS (III) shall provide the capability to apply response generation rules to define the content, media, and destination of the response. NGI-369

III will not limit the number of rules that apply to a response request.

SYS882 IAFIS (III) shall provide the capability to base response generation rules on the type of response (e.g., ten-print submission response).

SYS883 IAFIS (III) shall provide the capability to base response generation rules on the originator of request (e.g., ORI).

SYS884 IAFIS (III) shall provide the capability to base response generation rules on the results of the request (e.g., identification versus non-identification).

SYS885 IAFIS (III) shall provide the capability to base response generation rules on the type of originator (e.g., law enforcement organization versus non-law enforcement organization).

SYS886 IAFIS (III) shall provide the capability to base response generation rules on the purpose code of request (e.g., law enforcement purposes or security clearance purposes).

SYS887 IAFIS (III) shall provide the capability to base response generation rules on the state of originator (e.g., Florida, Vermont).

SYS888 IAFIS (III) shall provide the capability to base response generation rules on the subject included in the response (identified by unique identifier).

SYS889 IAFIS (III) shall provide the capability to base response generation rules on the individual arrest or civil cycles contained within the subject included in the response.

SYS890 IAFIS (III) shall provide the capability to create additional responses (messages to destinations not included in the request) based on a combination of response generation rules.

SYS891 IAFIS (III) shall allow contributors to indicate additional agencies that will automatically receive all identification responses.

SYS892 IAFIS (III) shall allow contributors to indicate additional agencies that will receive the response (whether identification or Non-Identification) for a given submission or search.

SYS893 IAFIS (III) shall provide the capability to suppress specific III/NFF unsolicited messages for individual states upon request.

3.7.8.3 National Fingerprint File Program Support

SYS894 IAFIS (III) shall provide the capability to create requests for data from National Fingerprint File (NFF) state databases according to III/NFF Operational and Technical Manual.

SYS895 IAFIS (III) shall provide the capability to retransmit the NFF criminal history request when the NFF state does not respond or the response is incomplete.

SYS896 IAFIS (III) shall provide the capability to adjust the number of times the NFF criminal history request is retransmitted for electronic criminal submissions.

SYS897 IAFIS (III) shall provide the capability to adjust the number of times the NFF criminal history request is retransmitted for electronic civil submissions.

SYS898 IAFIS (III) shall provide the capability to adjust the number of times the NFF criminal history request is retransmitted for all transactions other than electronic criminal or electronic civil submissions.

SYS899 IAFIS (III) shall provide the capability to define the retransmission interval for the NFF criminal history request from one to 60 minutes for electronic criminal submissions.

NGI-370

SYS900 IAFIS (III) shall provide the capability to define the retransmission interval for the NFF criminal history request from one to 99 hours for electronic civil submissions.

SYS901 IAFIS (III) shall provide the capability to define the retransmission interval for the NFF criminal history request from one to 99 hours for all transactions other than electronic criminal or electronic civil submissions.

SYS902 IAFIS (III) shall compile data received from NFF states, within the III criminal configurable parameters, with the data held in queue by III, into one electronic response for criminal EFTS transactions.

SYS903 IAFIS (III) shall compile data received from NFF states, within the III civil configurable parameters, with the data held in queue by III, into one electronic response for civil EFTS transactions.

SYS904 IAFIS (III) shall compile data received from NFF states, within the III other than electronic criminal or electronic civil configurable parameters, with the data held in queue by III, into one response, for non-EFTS transactions.

SYS905 IAFIS (III) shall provide all available data held by III when an NFF state does not respond in a timely manner.

SYS906 IAFIS (III) shall query the state system for the necessary criminal history information where ownership responsibility of the criminal history data resides with an NFF state.

SYS907 IAFIS (III) shall assemble the responses by the states where ownership responsibility of the criminal history data resides with an NFF state.

SYS908 IAFIS (III) shall forward the assembled responses to non-III requester states where ownership responsibility of the criminal history data resides with an NFF state.

3.7.8.4 Response Printing

SYS909 IAFIS (III) shall organize responses for printing into groups as defined in the III Software Design Document.

SYS910 IAFIS (III) shall have the capability to print groups automatically.

SYS911 IAFIS (III) shall be able to defer printing of hardcopy responses for a preset period (up to 12 hours).

SYS912 IAFIS (III) responses shall be grouped and printed to provide output distribution.

SYS913 IAFIS (III) shall use the Computerized Contributor Address File address table to determine the address for the response.

SYS914 IAFIS (III) shall print hardcopy responses with the appropriate destination name and address.

3.7.8.5 Response Media

SYS915 IAFIS (III) shall determine the type of media for the response based upon the type of submission (i.e., NCIC, EFTS external, EFTS/CSS, MRD).

IAFIS will return an electronic response for electronic inputs from authorized Contributors. IAFIS will print hardcopy responses for electronic inputs from the CSS and send an electronic completion message to the CSS.

SYS916 IAFIS (III) shall determine the type of media for the response by the instructions in the MRD ORI file, when the type of submission is MRD.

3.7.8.6 Receiving Agency Notification Report (RANR)

A Receiving Agency Notification Report (RANR) request will be requested by the ITN/DPS Service Provider to generate the list of all agencies receiving the rap sheet of a given FBI Number. RANR report will be generated by III. A RANR request will be entered and verified by ITN/DPS and then forwarded to III for information retrieval. Upon receiving responses from III, ITN/DPS will display the information and initiate a local hardcopy generation if desired.

SYS2297 IAFIS (III) shall provide the capability for an Authorized FBI Service Provider to request a Receiving Agency Notification Report (RANR) as part of the Criminal History Request.

SYS917 IAFIS (III) shall include, on the RANR, a list of agencies that have received the rap sheet for the given FBI number.

SYS918 IAFIS (III) shall use the CRS file to determine which agencies have received the rap sheet for the given FBI number.

Agencies that have made requests for the given record via NCIC or through FBI service providers will be logged in the CRS file.

SYS919 IAFIS (III) shall use the SCH record to determine which agencies have received the rap sheet for the given FBI number.

SYS920 IAFIS (III) shall apply the Response Generation Rules to the generation of the RANR.

Arrests posted within the last year would have resulted in a copy of the record being sent to the submitting agency and possibly that agency's state bureau.

SYS2298 IAFIS (III) shall provide the RANR when requested for the specified subject as part of the Criminal History Request response.

3.7.8.7 Record Set Report

SYS921 IAFIS (III) shall include all disseminable criminal history in the Record Set Report based on the authorization of the requesting Authorized FBI Service Provider.

SYS922 IAFIS (III) shall apply the Response Generation Rules to the generation of the Record Set Report.

3.7.9 File Maintenance

3.7.9.1 Photo File Maintenance

SYS923 ITN shall forward a Photo Add Request to III.

SYS924 IAFIS (III/IPS) shall store a criminal photo set as part of the Photo Add Request.

SYS925 IAFIS (III/IPS) shall add photo summary information to the criminal history record as part of an Photo Add Request.

The photo summary information will indicate that photos are on file in the IPS repository for the arrest cycle.

SYS926 IAFIS (III/IPS) shall maintain descriptive information about the criminal photo sets.

The criminal photo set will include the subset of the EFTS type-10 record, the date of arrest, and the date of arrest suffix.

3.7.9.2 Update Subject Criminal Record

SYS927 IAFIS (III) shall delete expired flash data from the subject's record when performing subject criminal history file maintenance.

SYS928 IAFIS (III) shall delete expired SOR data from the subject's record when performing subject criminal history file maintenance.

SYS929 IAFIS (III) shall record all transactions which caused subject criminal history changes to the kept FNU following a consolidation.

3.7.9.3 Create New IAFIS Records

SYS930 IAFIS shall enroll all Missing Persons and Unknown Deceased submissions that result in a non-identification decision into the criminal repositories.

SYS931 IAFIS shall enroll all Amnesia Victims retained submissions that result in a non-identification decision into the criminal repositories.

SYS932 IAFIS shall enroll all criminal retained submissions that result in a non-identification decision into the criminal repositories.

SYS933 IAFIS shall enroll all civil retained submissions (excluding Amnesia Victims, Missing Persons, and Unknown Deceased submissions) that result in a non-identification decision into the civil repositories.

SYS934 IAFIS (ITN) shall create a unique subject identifier (FNU or CRN) in accordance with the MDD as a result of a retained Ten-Print Fingerprint Identification Search Request that results in a non-identification decision.

SYS935 IAFIS (III) shall enroll subject criminal history information for the subject identifier (FNU or CRN) into the appropriate IAFIS repository as a result of a retained Ten-Print Fingerprint Identification Search Request that results in a non-identification decision.

SYS936 IAFIS (ITN/ISRE) shall enroll subject fingerprint image information for the subject identifier into the appropriate IAFIS repository based on file maintenance rules as a result of a retained Ten-Print Fingerprint Identification Search Request that results in a non-identification decision.

SYS937 IAFIS (AFIS) shall enroll subject fingerprint feature information for the subject identifier into the appropriate IAFIS repository based on file maintenance rules as a result of a retained Ten-Print Fingerprint Identification Search Request that results in a non-identification decision.

3.7.9.4 Update IAFIS Record

SYS938 IAFIS (III) shall update subject criminal history information based on file maintenance rules as a result of a Ten-Print Fingerprint Identification Search Request with an identification decision.

SYS939 IAFIS (AFIS) shall update fingerprint feature information based on file maintenance rules as a result of a Ten-Print Fingerprint Identification Search Request with an identification decision.

An automated repository update is an update transaction where the new image contains better characteristics quality information than the characteristics in the fingerprint repository.

SYS940 IAFIS (AFIS) shall perform an automated repository update of the fingerprint feature information as a low priority inter-segment transaction without impacting existing feature search processes.

SYS941 IAFIS (AFIS) shall retrieve data from the specified repository corresponding to a subject ID number provided and compare the characteristics quality information for each finger when performing an automated repository update.

SYS942 IAFIS (AFIS) shall update the fingerprint features with the new information when the characteristic quality information of the new image is better than the stored image.

SYS943 IAFIS (ITN) shall indicate that a forced feature update is necessary during file maintenance.

A forced feature update may result from fingerprint image replacement during FIC comparison functions.

SYS944 IAFIS (AFIS) shall perform a forced feature update of the fingerprint feature information contained in the file maintenance action.

SYS945 IAFIS (AFIS) shall replace features as part of a forced feature update resulting from a change in the fingerprint classification of an individual (i.e., through designation of a scar or amputation).

SYS946 IAFIS (AFIS) shall delete features from any SLC when the same features are deleted from CMF.

SYS947 IAFIS (ITN/ISRE) shall initiate an update fingerprint image information based on file maintenance rules as a result of a Ten-Print Fingerprint Identification Search Request with an identification decision.

The update fingerprint image information will contain an FBI Number, corresponding fingerprint images, and an ICN.

SYS948 IAFIS (III) shall establish a pointer (SID) when processing all criminal ten-print submissions that result in an identification when a SID does not exist on the record for the contributor, to support the III/NFF programs.

SYS949 IAFIS (III) shall establish a pointer (SID) when processing all criminal retained ten-print submissions that result in a non-identification, to support the III/NFF programs.

SYS950 IAFIS (ITN) shall store a copy of the submission in the Ten-Print Certification File for all criminal ten-print submissions. NGI-374

SYS951 IAFIS (ITN) shall store a copy of the submission in the Ten-Print Certification File for all civil ten-print submissions (military, federal employees, and state and local employees) that result in a criminal identification.

SYS952 IAFIS (III) shall maintain the following identification information for criminal records during processing of purges due to death notices: the FBI identification number, AUD code, date record entered, date last updated, time last updated, master name, sex, race, height, weight, eye color, hair color, city of birth, place of birth, state establishing record, the AFIS generated pattern level fingerprint classification, explanation, and III pointers.

3.7.9.5 Latent File Maintenance

SYS953 IAFIS (AFIS) shall delete the oldest record from the ULF, when the ULF is at maximum capacity and a new record is received for enrollment.

SYS954 AFIS shall send an image delete request to ITN when an image exists for a deleted ULF record.

SYS955 IAFIS (ITN/ISRE) shall receive ULF fingerprint image maintenance requests from ITN/LPS.

SYS956 IAFIS (AFIS) shall received ULF fingerprint feature maintenance request from ITN/LPS.

SYS957 IAFIS (ITN/LPS) shall apply a unique identification number for each image of a Latent Case retained in the FBI's files.

SYS958 IAFIS (ITN/LPS) shall use the LCN and its extensions (LCX) as a unique identifier.

SYS959 IAFIS (ITN/LPS) shall provide the capability to store latent search details.

SYS960 IAFIS (ITN/LPS) shall store latent search requests initiated by an Authorized FBI Latent Service Providers.

SYS961 IAFIS (ITN/LPS) shall provide the capability to retrieve latent searches.

SYS962 IAFIS (ITN/LPS) shall provide the capability to modify previously stored latent search parameters.

3.7.10 Cascaded Searches

SYS963 IAFIS (AFIS) shall perform a cascaded fingerprint search of the ULF as part of the enrollment of fingerprint information provided in a Ten-Print Fingerprint Identification Search Request.

SYS964 IAFIS (AFIS) shall perform a cascaded fingerprint search of the ULF as part of the update of fingerprint information resulting from a Ten-Print Fingerprint Identification Search Request, when appropriate.

SYS2159 IAFIS (ITN) shall perform a cascaded fingerprint search of the ULF when no identification was made from a criminal Ten-Print Fingerprint Identification Search Request.

SYS2160 IAFIS (ITN) shall perform a cascaded fingerprint search of the ULF when no identification was made from a humanitarian Ten-Print Fingerprint Identification Search Request.

NGI-375

SYS965 AFIS shall provide an Unsolved Latent Match (ULM) Notification to III when a Cascaded Fingerprint Search results in a potential match against a ULF record owned by an Authorized Contributor.

SYS966 IAFIS (III) shall process the ULM Notification according to the IAFIS ICD when the criminal history record contains a Special Processing Flag(s).

SYS967 III shall format an EFTS ULM Notification using the information provided by AFIS and forward the result to ITN when the ULM is being sent to an authorized Contributor.

SYS968 IAFIS (ITN/ISRE) shall retrieve the matching fingerprint image and the ULF candidate image information to be attached to the ULM Notification being sent to an authorized Contributor.

SYS969 AFIS shall provide an ULM Notification to ITN/LPS when a Cascaded Fingerprint Search results in a potential match against a ULF record owned by an Authorized FBI Service Provider.

The candidate information will consist of a combination of the ORI, the Contributor Case Identification Number (CIN), Contributor Case Identifier Extension (CIX), and the image.

3.7.11 User Fee Billing

IAFIS will collect User Fee History Data for IAFIS chargeable fingerprint and name search transactions. IAFIS will maintain administrative user fee data (tables, files, matrices) that support the calculation of user fees and generation of user fee bills. IAFIS will generate user fee bills and reports and provide capabilities to edit (correct) user fee bills. The history of producing the User Fee Billing Reports will be contained in the User Fee History Data.

SYS970 IAFIS (IDWH) shall provide Authorized FBI Service Providers access to user fee billing history, administrative, and billing data.

FBI Service Provider access to user fee history, administrative, and billing data will assist them in responding to user fee inquires from authorized user.

SYS971 IAFIS (IDWH) shall provide capabilities for Authorized FBI Service Providers to maintain (i.e., add, delete, modify) user fee administrative data.

3.7.11.1 Collect & Store User Fee Billing History Data

The user fee data necessary to support the user fee service will be supplied by the ITN and III segments. The ITN collects information from III along with its own information and makes it available to IDWH for processing. The ITN and III segments will perform the transaction processing functions, create a record containing data describing the results of such processing, and provide these records either directly or indirectly to IDWH. IDWH will collect and store user fee information for IAFIS chargeable fingerprint identification submissions and name check requests.

SYS972 IAFIS (ITN/TPS) shall collect User Fee Transaction data for user fee ten-print identification search transactions.

SYS973 IAFIS (ITN/DPS) shall collect User Fee Transaction data for user fee subject search transactions.

NGI-376

SYS974 IAFIS (III) shall collect User Fee Transaction data for user fee name search transactions.

III will collect at a minimum the following User Fee Transaction data: the date and time transaction received (by III), IAFIS Control Number, MRD rejecting code (if applicable), Originating Agency Identifier, Subject Name, date and time of transaction completion (by III), STOT, Type of Search Requested and the Contributor Assigned Identification Number.

SYS975 IAFIS (III) shall retain User Fee Transaction data for 14 days.

SYS976 ITN shall collect III User Fee Transaction data from III as defined in the IAFIS Database Specification Document.

SYS977 IDWH shall collect User Fee Transaction data from ITN as defined in the IAFIS Database Specification Document.

SYS978 IDWH shall collect the ITN User Fee Transaction data from ITN at regular intervals, and at a minimum of once within a 24 hour period.

SYS979 IAFIS (IDWH) shall recognize the following STOTs as User Fee transactions: DOCE, EMUF, FASS, FAUF, FIDO, FUFC, FOID, IFAUF, INFUF, NFAP, NFDP, NFFC, NFUE, NFUF, or SSRM.

SYS980 IAFIS (IDWH) shall extract User Fee Transaction data from User Fee Transaction that has completed processing in IAFIS.

SYS981 IAFIS (IDWH) shall consider a transaction completed if it has an IAFIS completion date/time assigned.

SYS982 IAFIS (IDWH) shall retain the original content of the User Fee Transaction data.

3.7.11.2 Process User Fee Transactions

SYS983 IAFIS (IDWH) shall allow an Authorized FBI System Administrator to initiate the User Fee Transaction Extract Transfer and Load (ETL) process.

SYS984 IAFIS (IDWH) shall identify a chargeable transaction from the User Fee Transaction data based on User Fee Business Rules.

IDWH will recognize a User Fee transaction as a valid chargeable transaction if it has a User Fee STOT, a completion date within IAFIS, the required fields are present (i.e., IAFIS Control Number (ICN), subject name, Controllers Agency Identifier (CRI), decision or reject reason), a Computerized Contributor Address (CCA) File compliant CRI or ORI, and valid, chargeable reject codes.

SYS985 IAFIS (IDWH) shall calculate a user fee rate for each chargeable transaction based on User Fee Business Rules.

SYS986 IAFIS (IDWH) shall identify billable user fee transactions as those transactions with the following STOTs: DOCE, EMUF, FASS, FAUF, FUFC, IFAUF, INFUF, NFFC, NFUE, NFUF, or SSRM.

SYS987 IAFIS (IDWH) shall assign an Account Receivable Number (ARN) to the billable User Fee Transactions.

SYS988 IAFIS (IDWH) shall create an entry in a User Fee Billing Process Exception Log if a

NGI-377

problem occurs that prevents the assignment of user fee rate, billing agency, and/or ARN.

SYS989 IAFIS (IDWH) shall provide to an Authorized FBI System Administrator the UFB ETL Process results.

The UFB ETL process results will include the total number of records processed, number of records processed successfully, and number of records identified with processing errors (UFB Filter errors and User Fee Billing Process Exceptions) upon completion of the UFB ETL Process.

3.7.11.3 User Fee Billing Process Exception File

SYS990 IAFIS (IDWH) shall maintain the User Fee Billing Process Exception Log.

The User Fee Billing Process Exception Log will contain, at a minimum, the User Fee Transaction data record, error code, literal error message, and the date and time the error entry was made.

SYS991 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Providers to query and view User Fee Billing Process Exceptions.

IDWH will allow Authorized FBI Service Providers the ability to query the UFB Exceptions File by CRI, Billing Agency, ICN, Subject Name, OCA, Transaction Date Completed, STOT, Decision, and Literal Error Message via the UFB Exceptions HMI.

SYS992 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Providers to print User Fee Billing Process Exception.

3.7.11.4 User Fee Business Rules

The User Fee Business Rules will be based on:

a. User fee rates;

b. Special rates based on transaction Originating Agency Identification (ORI);

c. Billing Agency;

d. Reason fingerprinted code (RFP);

e. Contributor Class Code (CCC);

f. Type of Search Requested (TSR); and

g. STOT.

SYS993 IAFIS (IDWH) shall store UFB Business Rules.

SYS994 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Provider to add User Fee Business rules.

SYS995 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Provider to modify User Fee Business rules.

SYS996 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Provider to delete User Fee Business rules.

SYS997 IAFIS (IDWH) shall store billing information for each chargeable agency in an ORI

file.

SYS998 IAFIS (IDWH) shall maintain billing information for each chargeable agency in an ORI file.

3.7.11.5 User Fee Pre-Payment Reporting

IAFIS supports two payment methods for user fee billing services: pre-payment and billing. For the pre-payment method, IAFIS utilizes three types of user fee transactions: Non-Federal Direct Payment, Non-Federal Pre-Payment, and Freedom of Information Act document.

Non-Federal Direct Payment transactions are Non-Federal user fee hardcopy fingerprint identification requests in which contributors attach a payment document for the fingerprint card processing fee. Non-Federal Pre-Payment transactions are user fee fingerprint identification requests in which contributors pre-pay via electronic funds transfer (i.e., PAY.GOV) for the fingerprint card processing fee. Freedom of Information Act requests are federally mandated fingerprint identification requests in which contributors attach the processing fee to the fingerprint card. IAFIS will not include these pre-payment transactions on any user fee bills or in calculation of billed revenue.

SYS999 IAFIS (IDWH) shall maintain user fee transaction summary data for user fee Direct Payment transactions (NFDP).

SYS1000 IAFIS (IDWH) shall produce Direct Payment reports for Direct Payment transactions (NFDP) as defined in the IDWH Software Design Document.

SYS1001 IAFIS (IDWH) shall maintain user fee transaction summary data for user fee Non-Federal Pre-Payment transactions (NFAP).

SYS1002 IAFIS (IDWH) shall produce Pre-Payment transaction reports for Non-Federal Pre-Payment transactions (NFAP) as defined in the IDWH Software Design Document.

SYS1003 IAFIS (IDWH) shall maintain user fee summary data for user fee Freedom of Information Act document transactions (DOCE, FIDO and FOID).

SYS1004 IAFIS (IDWH) shall produce Freedom of Information Act document transaction reports for Freedom of Information Act document transactions (DOCE, FIDO and FOID) as defined in the IDWH Software Design Document.

3.7.11.6 User Fee Billing Data Adjustments

An Authorized FBI Service Provider may review and adjust User Fee Billing data prior to and after the official generation of the user fee bills.

SYS1005 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Provider to view User Fee Billing data.

SYS1006 IAFIS (IDWH) shall provide the capability for an Authorized FBI Service Provider to make adjustments to User Fee Billing data as defined in the IDWH Software Design Document.

An Authorized FBI Service Provide may make adjustments to the following User Fee Billing data: user fee rate, ORI, ICN, billing date range (not to exceed thirteen months), Subject name, and TCN.

NGI-379

SYS1007 IAFIS (IDWH) shall display pre-billing cycle adjustments as a normal user fee

transaction on the bill as defined in the IDWH Software Design Document.

Pre-billing adjustments are those user fee billing data adjustments made during the billing cycle. A billing cycle is defined as 1 calendar month, starting on the 1st.

SYS1008 IAFIS (IDWH) shall generate a credit memo for all post-billing cycle adjustments made after a billing cycle, known as post-billing adjustments.

SYS1009 IAFIS (IDWH) shall provide the capability to generate credit memos against data up to 1 year after transaction completion.

SYS1010 IAFIS (IDWH) shall allow an authorized user to credit an incorrectly billed agency, and reassign the User Fee Transactions to the correct Billing Agency.

SYS1011 IAFIS (IDWH) shall provide a report of all billing adjustments made in a given month, due to an incorrect Billing Agency assignment.

3.7.11.7 No Charge Resubmissions

SYS1012 IAFIS (IDWH) shall maintain a record of all rejected chargeable submissions to support the processing of "no charge" resubmissions.

SYS1013 IAFIS (IDWH) shall ensure that a user fee is not applied ("no charge") for invalid resubmissions.

For submissions rejected due to unclassifiable fingerprint image(s), it is assumed that a name check has been performed with negative results. A fingerprint resubmission is validated based on the following conditions:

a. for hardcopy fingerprint submissions, the originally rejected (unclassifiable) fingerprint card must accompany the new fingerprint card;

b. for electronic fingerprint submissions, the original submission's TCN must be present in the No Charge Indicator field, and the IAFIS assigned ICN for the original submission must be in the Type-1 TCR (Transaction Control Reference) field for the resubmission;

c. for all resubmission, the textual data for the original and resubmission must be identical, such as ORI, Reason Fingerprinted, and name; and

d. for all resubmissions, only 1 resubmission is permitted for "no charge" processing. If the resubmission is again rejected, the contributor will be billed for any subsequent resubmission.

3.7.11.8 User Fee Billing Change History Data

SYS1014 IAFIS (IDWH) shall provide a form for the Authorized FBI Service Provider entry of User Fee Billing adjustment data.

SYS1015 IAFIS (IDWH) shall store the change history data related to the creation and adjustment of a billing record.

SYS1016 IAFIS (IDWH) shall store the original user fee charged amount, the adjusted user fee amount, the date and time of the change, the Employee Identifier (EID) of the employee who made the change, and the reason for the User Fee Billing adjustment.

SYS1017 IAFIS (IDWH) shall provide the capability to generate pre-defined and ad hoc reports

to support the management and administration of the user fee program.

SYS1018 IAFIS (IDWH) shall output User Fee Administrative reports and query results in hardcopy, displayed on-line, or saved to an electronic file.

3.7.11.9 Maintain User Fee Billing Data Accuracy

SYS1019 IAFIS (IDWH) shall retain the accuracy and granularity of all User Fee Billing data as originally received.

SYS1020 IAFIS (IDWH) shall protect all User Fee Billing data from unauthorized modification (i.e., ensure that the data and information remain as received unless changed through authorized processes and procedures).

SYS1021 IAFIS (IDWH) shall provide a journaling capability to allow restoration of a consistent collection of User Fee Billing data from an established baseline.

SYS1022 IAFIS (IDWH) shall ensure User Fee Billing data integrity at the field level.

SYS1023 IAFIS (IDWH) shall provide the capability to ensure referential integrity of User Fee field values across multiple tables/records in the database (e.g., triggers).

3.7.11.10 Maintain User Fee Rate and User Fee Billing Tables

SYS1024 IAFIS (IDWH) shall maintain User Fee Administrative Data.

SYS1025 IAFIS (IDWH) shall maintain User Fee rate tables which indicate rates by contributor type (Federal and Non-Federal), by submission type (fingerprint identification or name check request), by submission media (hardcopy, paper request or electronic), and by reason for submission.

SYS1026 IAFIS (IDWH) shall maintain User Fee billing tables which contain contributor and channeling agency information as to whom to bill, where to send the bill, and in what format (hardcopy) the bills should be sent (e.g., Federal User Fee Reporting Matrix).

3.7.11.11 User Fee Billing Queries and Reports

SYS1027 IAFIS (IDWH) shall support the management of Authorized FBI Service Provider User Fee Billing queries, reports, and forms.

SYS1028 IAFIS (IDWH) shall support the integration of developed User Fee Billing scripts, reports, and forms in the user interface.

SYS1029 IAFIS (IDWH) shall allow Authorized FBI Service Providers to substitute pre-defined User Fee Billing reports.

SYS1030 IAFIS (IDWH) shall allow Authorized FBI Service Providers to name, rename, save, retrieve, delete, and print User Fee Billing reports.

SYS1031 IAFIS (IDWH) shall allow Authorized FBI Service Providers to name, rename, save, retrieve, delete, and print User Fee Billing forms.

SYS1032 IAFIS (IDWH) shall allow Authorized FBI Service Providers to name, rename, save, retrieve, delete, and print User Fee Billing operating system control scripts.

SYS1033 IAFIS (IDWH) shall allow Authorized FBI Service Providers to direct the output of

User Fee Billing reports, forms, or scripts to the workstation display, files, or printers.

SYS1034 IAFIS (IDWH) shall provide User Fee Billing reports and query results to ITN workstations.

SYS1035 IAFIS (IDWH) shall produce User Fee Billing output in pre-defined formats, ASCII, and formats compatible with the current CJIS standard spreadsheet and word processor.

SYS1036 IAFIS (IDWH) shall provide pre-defined User Fee Billing reports for an established period such as weekly, 10-day, 14-day, monthly, quarterly, fiscal year, and calendar year.

The established periods will be identified as follows:

a. weekly—Sunday through Saturday;

b. 10-day—ten consecutive workdays (excluding Saturday and Sunday);

c. 14-day—14 consecutive days (including Saturday and Sunday);

d. monthly—from the first day of the month through the last day of the month;

e. quarterly—from the first day of the first month through the last day of the last month of the quarter;

f. fiscal year—October 1 through September 30; and

g. Calendar year—January 1 through December 31.

SYS1037 IAFIS (IDWH) shall maintain on-demand or automatic search queries for each User Fee Billing report that defines the Period of Report (i.e., Daily, Weekly, every 10-days, Monthly, Yearly, as well as other user or operator-defined time periods).

SYS1038 IAFIS (IDWH) shall provide automatic User Fee Billing reports which are produced as part of a report set (i.e., Daily, Weekly, Monthly, or Yearly) or upon user or operator request for a specified time period.

SYS1039 IAFIS (IDWH) shall provide on-demand User Fee Billing reports to be individually produced by authorized user or operator as requested for a specified time period.

SYS1040 IAFIS (IDWH) shall also provide for the capability to produce and distribute any automatic User Fee Billing report for a specified time period.

SYS1041 IAFIS (IDWH) shall provide authorized operators the capability to modify User Fee Billing report formats and to create new User Fee Billing report formats.

SYS1042 IAFIS (IDWH) shall provide the capability to store generated automatic User Fee Billing reports in a central repository, allowing users and operators to access the automatic reports instead of generating the same report multiple times.

SYS1043 IAFIS (IDWH) shall allow authorized operators to adjust the retention duration for categories of User Fee Billing reports.

3.7.11.12 Ad Hoc Query Capability

SYS1044 IAFIS (IDWH) shall provide the capability to generate ad hoc reports to support the management and administration of the user fee program.

SYS1045 IAFIS (IDWH) shall provide an ad hoc query capability to support the analysis of data contained in the databases related to user fee activity.

SYS1046 IAFIS (IDWH) shall provide reports and query User Fee Billing results in hardcopy, displayed on-line, or saved to an electronic file.

3.7.11.13 Data Thresholds and Collection Parameters

SYS1047 IAFIS (IDWH) shall provide the capability for authorized operators to establish User Fee Billing processing thresholds.

SYS1048 IAFIS (IDWH) shall abort User Fee Billing requests that exceed set processing thresholds.

SYS1049 IAFIS (IDWH) shall notify an operator when a User Fee Billing processing is aborted and include the reason for the abort.

SYS1050 IAFIS (IDWH) shall allow authorized operators to change User Fee Billing data collection parameters without requiring system re-boot.

SYS1051 IAFIS (IDWH) shall allow authorized operators to change the total records returned in any one User Fee Billing query.

SYS1052 IAFIS (IDWH) shall allow authorized operators to change the total time used by any one User Fee Billing query.

SYS1053 IAFIS (IDWH) shall allow authorized operators to change the number of active User Fee Billing query processes.

3.7.11.14 User Fee Bill Generation

SYS1054 IAFIS (IDWH) shall print hardcopy bills with the appropriate destination name, address, and calculations of user fee transactions.

SYS1055 IAFIS (IDWH) shall provide the capability to produce user fee bills in electronic (softcopy) format with the appropriate destination.

SYS1056 IAFIS (IDWH) shall generate user fee activity reports to support the CJIS Division Financial Management Unit Audits.

SYS1057 IAFIS (IDWH) shall have the capability to create bills based on User Fee Business Rules.

SYS1058 IAFIS (IDWH) shall have the capability to print user fee billing information.

SYS1059 IAFIS (IDWH) shall have the capability to print complete user fee bills by ORI, ARN, or Billing Agency from an HMI.

SYS1060 IAFIS (IDWH) shall have the capability to regenerate all or specific bills by ORI, ARN, or Billing Agency from an HMI.

SYS1061 IAFIS (IDWH) shall have the capability to print audit history logs, UFB error, and UFB exception logs.

SYS1062 IAFIS (IDWH) shall have the capability to print all user fee transaction loading rejections.

SYS1063 IAFIS (IDWH) shall have the capability to not bill for rejections in QC function.

SYS1064 IAFIS (IDWH) shall have the capability to store, retrieve, and display user fee bills.

3.7.11.15 Create Hardcopy Bills

SYS1065 IAFIS (IDWH) shall provide the capability to create black and white hardcopy user fee bills.

SYS1066 IAFIS (IDWH) shall provide the capability to create color hardcopy user fee bills.

SYS1067 IAFIS (IDWH) shall provide user fee billing printer capabilities that include support for all printable ASCII characters and symbols.

SYS1068 IAFIS (IDWH) shall provide user fee billing printer capabilities that include standard, scalable, and proportional fonts in variable point sizes and standards.

SYS1069 IAFIS (IDWH) shall provide user fee billing printer capabilities that include print Density: minimum 300 by 300 dots per inch, for text and graphics.

SYS1070 IAFIS (IDWH) shall provide user fee billing printer capabilities that include landscape and portrait capabilities as a software selectable user option.

SYS1071 IAFIS (IDWH) shall provide user fee billing printer capabilities that support user-selectable dual-sided (Duplex) printing.

SYS1072 IAFIS (IDWH) shall support the capability to print at least 20 pages per minute for black and white 11 x 17 size paper for user fee bills.

SYS1073 IAFIS (IDWH) shall support the capability to print at least five (5) pages per minute for color 8 ½ x 11 size paper for user fee bills.

3.7.11.16 Create Federal Bills

SYS1074 IAFIS (IDWH) shall generate federal electronic and hardcopy bills.

SYS1075 IAFIS (IDWH) shall generate the federal user fee bill containing the User Fee Bill Totals, the Central Agency Summary, a Return Page, an ORI Detail Listing, and an ORI Summary.

3.7.11.17 Create Non-Federal Bills

SYS1076 IAFIS (IDWH) shall generate non-federal electronic and hardcopy bills.

SYS1077 IAFIS (IDWH) shall generate the non-federal user fee bill containing the User Fee Bill Totals, a Central Agency Summary, a Return Page, an ORI Detail Listing, and an ORI Summary.

3.7.11.18 Supplemental Bill Generation

SYS1078 IAFIS (IDWH) shall allow an Authorized FBI Service Provider to generate a supplemental bill for the correct Billing Agency which includes the mis-billed transaction information when the wrong agency was billed.

SYS1079 IAFIS (IDWH) shall provide a supplemental bill that contains a Central Agency Summary page, Remittance Page, and ORI Detail Summary.

SYS1080 IAFIS (IDWH) shall provide the capability to generate supplemental bills for up to 1 year after the original bill generation.

NGI-384

3.7.11.19 Support Data Archival

SYS1081 IAFIS (IDWH) shall have the capability to store on-line User Fee History Data for two full physical years.

SYS1082 IAFIS (IDWH) shall have the capability for online retrieval of up to 6 months of archived, replicated, and historical IAFIS system transaction data (UFB data) in addition to the 2 full years of online storage.

SYS1083 IAFIS (IDWH) shall have the capability for on-line retrieval of up to 6 months of archived UFB data in addition to the 3 years of on-line storage.

SYS1084 IAFIS (IDWH) shall have the capability to make readily available and retrievable the archived UFB data by individual monthly increments for up to 6 months.

SYS1085 IAFIS (IDWH) shall have the capability to archive and provide off-line storage of all replicated UFB data for 4 years 3 months.

SYS1086 IAFIS (IDWH) shall combine the UFB data on-line and off-line storage for a duration of 6 years 3 months.

SYS1087 IAFIS (IDWH) shall generate two copies of the archived user fee billing data, one copy stored at CJIS Clarksburg West Virginia Complex and one copy stored off-site.

SYS1088 IAFIS (IDWH) shall store the User Fee Transaction (UFT) data, bills, logs, and change history data related to the creation and adjustment of a billing record (bill) on-line for two full fiscal years.

SYS1089 IAFIS (IDWH) shall maintain user fee billing data for a total of seven (7) years.

SYS1090 IAFIS (IDWH) shall allow authorized operators to adjust the on-line user fee billing data retention durations by data categories identified in Tables 3.7.11-1.

Each specific data type's on-line data retention period, as shown in Tables 3.7.11-1, will be added to an off-line data retention period, to total seven (7) years.

Table 3.7.11-1 IAFIS Record On-Line Retention Duration

Records	On-Line Retention Duration
ITN Input Data	
Ten Print Services User Fee Data	13 months
Document Services (FASS)	13 months
III Input Data	
Automated Name Search Services User Fee Data	13 months
Computerized Contributor Address (CCA) File	13 months

SYS1091 IAFIS (IDWH) shall provide the capability for authorized operators to transfer on-line data to off-line media using a format and mechanism which is directly compatible with the UFBS off-line to on-line data transfer capability.

SYS1092 IAFIS (IDWH) shall allow authorized operators to select user fee billing data to be transferred off-line by environment (operational, test, maintenance/development, or training), filename(s), and time periods.

SYS1093 IAFIS (IDWH) shall provide the capability to restore user fee billing data stored off-line, regardless of the environment from which it was originally transferred. (Note: only

operational data will be provided to the operational environment).

SYS1094 IAFIS (IDWH) shall provide a user fee billing archive/retrieve response with an affirmative or a rejection that includes the reason for rejection.

SYS1095 IAFIS (IDWH) shall provide an archiving process that will not degrade the UFB performance below the stated response time requirements.

3.7.11.20 File Administration

SYS1096 IAFIS (IDWH) shall provide the capability for authorized operators to perform user fee billing file loading.

SYS1097 IAFIS (IDWH) shall provide the capability for authorized operators to perform user fee billing file transfers.

SYS1098 IAFIS (IDWH) shall provide the capability for authorized operators to perform user fee billing backups and recovery.

3.7.11.21 Backup and Recovery Services

SYS1099 IAFIS (IDWH) shall provide the capability to backup, on bulk media, and restore complete and partial copies of the user fee billing database, the system files, any data files, the system software, and the application software.

SYS1100 IAFIS (IDWH) shall provide user fee billing backup and recovery both automatically at authorized operator-specified intervals and on-demand by authorized operators.

SYS1101 IAFIS (IDWH) shall generate backups that will not degrade the UFB performance below the stated response time requirements.

SYS1102 IAFIS (IDWH) shall allow authorized operators to adjust user fee billing data retention durations by data types, and adjust backup recovery and archival frequencies by data types.

3.7.11.22 Data Analysis Tools

SYS1103 IAFIS (IDWH) shall provide data analysis tools for manipulating, measuring, and analyzing user fee billing data.

SYS1104 IAFIS (IDWH) shall provide UFB data analysis tools which allow users to process user fee data and compare data, derive trends, and identify data relationships.

SYS1105 IAFIS (IDWH) shall provide UFB data analysis tool set to include data manipulation capability to sort, combine, move, copy, and aggregate data.

SYS1106 IAFIS (IDWH) shall provide UFB data analysis tool set to include analytical tools and routines to perform statistical and trend analysis.

SYS1107 IAFIS (IDWH) shall provide UFB data analysis tool set to include graphical analysis tools that provide plotting, charting, and histograms that include the mean, median, and norm segment processing times by type of transaction, segment transaction load, hour of day, day of week, and day of month.

SYS1108 IAFIS (IDWH) shall provide UFB data analysis tool set to include tools to compare transaction parameters and compare a transaction or a group of transactions with the mean, median, and norm values of any other group of transactions.

SYS1109 IAFIS (IDWH) shall provide the capability to present and store the results from the UFB data analysis tool set on-line.

SYS1110 IAFIS (IDWH) shall provide the capability to present the results from the UFB data analysis tool within an integrated report.

SYS1111 IAFIS (IDWH) shall provide the capability to store the results from the UFB data analysis tool on bulk media.

SYS1112 IAFIS (IDWH) shall provide the capability to print the results from the UFB data analysis tool.

3.7.11.23 Database Management

SYS1113 IAFIS (IDWH) shall provide the ability to add user fee billing data to the database.

SYS1114 IAFIS (IDWH) shall provide the ability to retrieve user fee billing data from to the database.

SYS1115 IAFIS (IDWH) shall provide the ability to update user fee billing data in the database.

SYS1116 IAFIS (IDWH) shall provide the ability to delete user fee billing data from the database.

SYS1117 IAFIS (IDWH) shall provide the ability to reorganize the user fee billing database (e.g., sort, join).

SYS1118 IAFIS (IDWH) shall verify that all user fee billing maintenance requests are valid and consistent with assigned access privileges prior to processing the requests.

SYS1119 IAFIS (IDWH) shall maintain all database maintenance responses for UFB that are either affirmative or rejection that includes the reason for rejection.

3.7.11.24 User Fee Billing Accounts

SYS1120 IAFIS (IDWH) shall provide 10 accounts to access UFB via IAFIS Workstations.

SYS1121 IAFIS (IDWH) shall be capable of supporting 10 IAFIS Workstation account logons with 10 simultaneous interactive sessions, providing this aggregate workload per minute described in Table 3.7.11-2.

Table 3.7.11-2 UFBS Aggregate Processing Workload

Task/Process	Activities per minute
ITN/UFBS	
Report Request	2
Report Definition/Modification	1
Simple Query[1]	2
Complex Query[2]	1
Security Audit	1
TOTALS	**7**

1 As defined in Table B-5.
2 Any query not defined as "simple" in Table 3-34 and Table 3-35.

NGI-387

3.7.11.25 User Fee Billing Workstations

UFB Workstations are those required to support UFB and are directly connected to the ITN segment containing all the functionality of the IAFIS Workstations.

SYS1122 IAFIS (IDWH) shall support distribution of the UFB application upgrade(s) on a minimum of 10 IAFIS Workstations.

SYS1123 IAFIS (ITN/TPS) shall provide access to the specified functionality for UFB via the IAFIS Workstation.

SYS1124 IAFIS (IDWH) shall support user fee billing access to the Operational Environment (OE) via IAFIS workstations.

SYS1125 IAFIS (IDWH) shall support user fee billing access to the Non-Operational (NOE Test) via IAFIS workstations.

SYS1126 IAFIS (IDWH) shall support user fee billing access to the Software Development Environment (SDE) via IAFIS workstations.

SYS1127 IAFIS (IDWH) shall support the queuing and printing of any user fee billing data (text and/or image) displayed on the IAFIS Workstation.

SYS1128 IAFIS (IDWH) shall use other existing IAFIS printer resources (e.g. ITN printers, III high speed printers) for user fee billing print capabilities.

3.7.11.26 Human Machine Interface

SYS1129 IAFIS (IDWH) shall provide an HMI on all IAFIS Workstations accessing UFB to allow the identification, selection, and execution of UFB functions and the entry and manipulation of UFB data.

SYS1130 IAFIS (IDWH) shall provide UFB HMIs to contain windows, icons, and pull-down menus as part of a Graphical User Interface (GUI) which is compatible with commercial guidelines for designing user interfaces for Windows-based applications.

3.7.11.27 Display Forms and Query Results

SYS1131 IAFIS (IDWH) shall include the capability for the authorized operator to add parameters to, and delete parameters from the previous user fee billing query to refine the results list for each presentation of results.

SYS1132 IAFIS (IDWH) shall have the capability to include the user fee billing query, the query results, and the number of items retrieved in response to a query.

SYS1133 IAFIS (IDWH) shall provide UFB HMIs with the capability to produce text and graphical data (to include standard business graphics such as bar, line, and pie charts).

SYS1134 IAFIS (IDWH) shall provide UFB HMIs with a full screen entry form generator capable of generating forms for on-line manual entry and review of operations and user fee billing data respectively, as well as the generation of queries and ad-hoc reports.

SYS1135 IAFIS (IDWH) shall provide UFB HMIs with visually identified functions available to individual operators based on assigned permissions.

SYS1136 IAFIS (IDWH) shall provide the capability for authorized operators to develop user

fee billing queries, reports, or forms, and test against a representative database for non-operational environments.

3.8 Administrative and Control Services

The following section contains the functional requirements relating to the specific areas of the administrative and control functions of IAFIS.

3.8.1 Communications

3.8.1.1 System Interfaces

SYS1137 IAFIS (EFCON) shall provide an interface to the CJIS WAN.

SYS1138 IAFIS (EFCON) shall process all CJIS WAN transactions in accordance with the latest Electronic Fingerprint Transmission Specification (EFTS).

SYS1139 IAFIS (EFCON) shall provide the capability to support batch processing from physical media data sources.

SYS1140 IAFIS (EFCON) shall provide the capability to support batch processing from file data sources.

SYS1141 IAFIS (III) shall provide an interface with the MRD process.

SYS1142 IAFIS (III) shall process all MRD transactions in accordance with the MRD Processing Manual.

SYS1143 IAFIS shall provide an interface with the interim Data Sharing Model (iDSM) using protocols specified in the IAFIS ICD.

SYS1144 IAFIS (III) shall provide an interface to NCIC in support of III/NFF state messaging.

SYS1145 IAFIS (III) shall process all III/NFF messages in accordance with the III/NFF Operations and Technical Manual.

IAFIS (III) uses the NCIC network to communicate with its external III users. Messages received by NCIC that contain an III header (2L01) are immediately routed to the III segment of IAFIS for processing. This interface is implemented with multiple TCP/IP socket connections. Incoming messages are received on one socket, and an asynchronous response is sent on a separate socket after processing completes.

SYS1146 IAFIS (III) shall support the use of an interface header on all III messages received via NCIC.

SYS1147 IAFIS (III) shall support the use of an interface header on all III responses returned to requestors via the NCIC network.

SYS1148 IAFIS (III) shall support the use of an interface header on all III unsolicited messages that are delivered via the NCIC network.

The interface header allows III to indicate to NCIC which logical line to use when sending the message. Message blocking characteristics and line number assignment for contributors are determined from the NCIC Line File maintained in III.

SYS1149 IAFIS (III) shall support an interface to NCIC in accordance with the NCIC Operating Manual.

IAFIS (III) also maintains an interface to NCIC as an NCIC "customer". This is also a TCP/IP socket connection, but unlike the III messaging this connection is synchronous. Hot Check requests are sent to NCIC on this connection and a synchronous response is received on the same socket. In addition, NCIC requires each user to support an asynchronous listener for the purpose of receiving unsolicited and administrative messages.

SYS1150 IAFIS (III) shall support an interface to Nlets in accordance with the Nlets Users Guide.

IAFIS (III) communicates with Nlets for the purpose of delivering XML rap sheets to the originators of III Criminal History requests (QR messages). Though the requests are received via the NCIC network, when III has criminal history information to share it is returned via Nlets in conformance with the Standardized Rap Sheet XML format. Nlets performs the service of either transforming this XML into standardized plain text, or pushing the XML all the way back to original requestor, depending on the capabilities of the requestor.

SYS1151 IAFIS (III) shall provide a communications interface to the FBI Special Functions system.

SYS2215 IAFIS shall provide an interface to iDSM in support of shared data.

SYS2216 IAFIS (iDSM) shall support an interface to the IDENT System.

SYS2217 IAFIS (iDSM) shall support an interface to the LESC System.

SYS2218 IAFIS will access DHS biographical information via a DHS established connection.

SYS2219 IAFIS (iDSM) shall support a CJIS Shared Storage Component (SSC/FBI) at the DOJ/DHS data center in the Rockville, MD Facility.

SYS2220 IAFIS (iDSM) shall support the main suite components (i.e., servers, terminals) in the CJIS Data Center at Clarksburg, WV.

The FBI will provide space for the DHS Shared Storage Component (SSC/DHS) at the CJIS Clarksburg, WV facility.

SYS2221 IAFIS shall support an internal interface to the CJIS Storage Area Network (SAN), also referred to as ESAN.

3.8.1.2 CJIS WAN Communications Management

The FBI will provide connectivity between the IAFIS facility and each state CSA via the CJIS WAN. This connectivity will be provided through Frame Relay services. The FBI will acquire the Frame Relay services for connecting state CSAs and IDENT Bureaus to the IAFIS for EFTS messages. Frame Relay will allow the EFCON to receive an aggregate workload from the states over the Frame Relay packet switch network through the IAFIS Firewall. The number of DTSs required at the EFCON will be the aggregate EFTS workload distributed over an appropriate number of T1 lines plus overhead and spares for EFTS traffic sized for a year 2012 workload.

NGI-590

SYS1152 IAFIS (EFCON) shall communicate with Authorized Contributors via the CJIS WAN using the protocols specified in the IAFIS ICD.

EFCON will support the Multipart Internet Mail Extensions (MIME) to SMTP in compliance with Internet Request for Comments 1521 and 1522 as outlined in the IAFIS ICD.

SYS1153 IAFIS (EFCON) shall support simultaneous delivery and receipt of electronic mail by multiple users.

SYS1154 EFCON shall determine EFTS compliance and reformat the transaction, if possible, before forwarding the transaction to ITN.

SYS1155 IAFIS (EFCON) shall record and report all formatting errors that cannot be automatically corrected.

SYS1156 IAFIS (EFCON) shall record all processing errors.

The EFCON System Transaction Validation function is responsible for the detection and related processing of errors in messages.

SYS1157 EFCON shall reject transactions to the submitting agency when the transaction cannot be forwarded to ITN.

SYS1158 EFCON shall pass incoming messages to ITN for processing via HTTP.

SYS1159 ITN shall route transaction responses to EFCON via HTTP for return to the submitting agency.

SYS1160 EFCON shall provide the capability to hold incoming messages for later delivery to ITN.

SYS1161 IAFIS (EFCON) shall provide the capability to hold outgoing messages for later delivery to CJIS WAN users.

SYS1162 IAFIS (EFCON) capacity shall be sufficient to hold 12 times the peak hour message traffic.

SYS1163 IAFIS (EFCON) shall provide the capability to automatically suspend EFCON processing of single or multiple transactions using predefined criteria, without human intervention.

SYS1164 IAFIS (EFCON) shall provide the capability to automatically resume EFCON processing of suspended system transactions using predefined criteria, without human interaction.

SYS1165 IAFIS (EFCON) shall maintain the ORI table which contains the Agency name and city along with the allowable functionality for each type of ORI.

SYS2222 IAFIS shall support a firewall implementation that prohibits offering general network file and print services to the user community.

SYS2223 IAFIS (iDSM) shall support a firewall implementation that is selected from the Common Criteria Evaluation and Validation Scheme (CCEVS) Validated Products List.

SYS2224 IAFIS (iDSM) shall support a router implementation that is external to the firewalls and independent of network routers or configurations with internal routers.

NGI-391

3.8.1.3 NCIC Communications Management

SYS1166 IAFIS (III) shall use the ORI File to validate the originator of an incoming NCIC message.

SYS1167 IAFIS (III) shall use the Line File to validate the NCIC Line Number of an incoming NCIC message and to route NCIC responses.

SYS1168 IAFIS (III) shall send Want Notifications to the NCIC logical line that corresponds to the Nlets system.

SYS1169 IAFIS (III) shall send SOR Notifications to the NCIC logical line that corresponds to the Nlets system.

SYS1170 IAFIS (III) shall provide the capability to hold outgoing messages for later delivery to NCIC.

3.8.1.4 Nlets Communications Management

SYS1171 IAFIS (III) shall communicate with Authorized Contributors via Nlets using the protocols specified in the IAFIS ICD.

3.8.1.5 Internal IAFIS Communications Management

SYS1172 IAFIS shall provide inter-segment connectivity between the IAFIS segments that allows traffic to pass between EFCON, ITN, AFIS, III, and IDWH.

The ITN Backbone Communications Element (BCE) provides the connectivity between the IAFIS segments.

SYS1173 IAFIS (ITN/BCE) shall comply with the standards identified in the IAFIS Target Architecture Document and the IAFIS ICD.

Note: The IAFIS ICD provides a detailed discussion of IAFIS interfaces and defines the physical connectivity and interface requirements between the segments.

SYS1174 IAFIS (ITN/BCE) shall support simultaneous communications between any combination of segments, elements, or sub-elements.

SYS1175 IAFIS (ITN/BCE) shall support communications between IAFIS Workstations and IAFIS segments.

SYS1176 IAFIS (ITN/BCE) shall allow local and remote operation and administration of all ITN/BCE equipment.

SYS1177 IAFIS shall monitor and report the status of internal communications.

SYS1178 IAFIS (ITN/BCE) shall maintain status information on all communications links between all segments and internal to ITN.

3.8.2 Data Management

This section provides all functional requirements specific to the data management of the IAFIS.

3.8.2.1 IAFIS Access Authorization Rules

Access to IAFIS repository files will be controlled based on a set of authorization rules. IAFIS will provide the capability to add, delete, and modify these authorization rules.

SYS1179 IAFIS (III) shall maintain authorization rules (i.e., read/write/delete access) for all Subject Criminal History activities.

SYS1180 IAFIS (ITN/TPS) shall maintain authorization rules (i.e., read/write/delete access) for all Fingerprint maintenance activities.

SYS1181 SYS1174 IAFIS (ITN/LPS) shall maintain authorization rules (i.e., read/write/delete access) for all Latent maintenance activities.

SYS1182 IAFIS (ITN/LPS) shall assign ownership of Latent File records.

Latent file ownership can be assigned to Authorized FBI Service Providers or Authorized Contributors. Ownership data will include: the ICN, the Case Number, Case Extension, the ORI, the CRI, and for FBI-owned records, the employee identifier (EID).

SYS1183 IAFIS (III) shall determine if the data service request is valid using the ORI, Type of Transaction, and Purpose Code.

SYS1184 IAFIS (III) shall retrieve the information from the requested file(s) when the data service request is valid.

3.8.2.2 IAFIS Dissemination Rules

SYS1185 IAFIS shall apply dissemination rules to all IAFIS notifications.

SYS1186 IAFIS shall apply dissemination rules to all IAFIS responses.

SYS1187 IAFIS shall maintain dissemination rules for all Subject Criminal History responses.

SYS1188 IAFIS (III) shall disseminate NFF and III states sealed records consistent with dissemination rules used for criminal history data stored in the Subject Criminal History File.

SYS1189 IAFIS (III) shall provide the dissemination of sealed data based upon the purpose of the request and the sealing dissemination criteria.

SYS1190 IAFIS shall maintain dissemination rules for all fingerprint responses.

SYS1191 IAFIS shall maintain dissemination rules for all Latent responses.

3.8.2.3 Subject Criminal History Data Management

SYS1192 IAFIS (III) shall support the synchronization of III subject criminal history data in accordance with the III Operations and Technical Manual.

SYS1193 IAFIS (III) shall provide the Segment Administrator the capability to produce III/NFF File Synchronization Tapes.

A periodic III Subject Criminal History data synchronization will be conducted with state systems to ensure that data is consistent with the FBI systems. IAFIS data for specific states will be made available periodically via magnetic media or FTP for this synchronization process.

SYS1194 IAFIS (III) shall provide the Segment Administrator the capability to produce the

Computerized Criminal History (CCH) Correlation Tape as specified in the III/NFF Operational and Technical Manual.

III will be capable of collecting all arrest, court, and custodial event information for a given state and time period. This information is written to tape and provided to the state for the purpose of bringing their criminal history system in sync with III. This process is referred to as CCH Correlation.

SYS1195 IAFIS (III) shall provide the capability to store multiple occurrences of name for a single subject.

SYS1196 IAFIS (III) shall provide the capability to store multiple occurrences of Social Security Number for a single subject.

SYS1197 IAFIS (III) shall provide the capability to store multiple occurrences of State Identification Number (SID) for a single subject.

SYS1198 IAFIS (III) shall provide the capability to store multiple occurrences of Scars, Marks, and Tattoos for a single subject.

SYS1199 IAFIS (III) shall provide the capability to store multiple occurrences of Miscellaneous Number for a single subject.

SYS1200 IAFIS (III) shall provide the capability to store multiple occurrences of Date of Birth (DOB) for a single subject.

3.8.2.4 Computerized Contributor Address File (CCA) Maintenance

SYS1201 IAFIS (III) shall maintain the Computerized Contributor Address File which contains contributor data (e.g., electronic and physical addresses) for Authorized Contributors.

The contributor data will be used for validation of incoming transactions and dissemination of responses.

SYS1202 IAFIS (III) shall support the association of discontinued (retired) Contributor identifiers to another active Contributor records in the IAFIS CCA File.

SYS1203 IAFIS (III) shall provide electronic responses to Authorized Contributors using contributor data (e.g., e-mail address) contained within IAFIS CCA File.

SYS1204 IAFIS (III) shall generate hardcopy responses to Authorized Contributors using contributor data (e.g., mailing address) contained within IAFIS CCA File.

IAFIS will use the stored contributor data to verify the required destination when preparing responses to IAFIS submissions. These responses may be either electronic or hardcopy depending upon the individual contributors needs. IAFIS will determine if the contributor can accept electronic or hardcopy responses and transmit the responses accordingly. If hardcopy responses are required, the resolution of the hardcopy will be of sufficient quality to meet ten-print fingerprint image comparison requirements.

SYS1205 IAFIS shall maintain a copy of the IAFIS CCA file in ITN.

SYS1206 IAFIS shall maintain a copy of the IAFIS CCA file in III.

3.8.2.5 Computerized Records Sent File Maintenance

SYS1207 IAFIS (III) shall store all the necessary information in Computerized Records Sent File in order to support the generation of the Receiving Agency Notification Report.

SYS1208 IAFIS (III) shall retain Computerized Records Sent File information on-line for one year and then retain the information off-line for nine years.

SYS1209 IAFIS (III) shall store off-line Computerized Records Sent File on removable media.

3.8.2.6 NCIC ORI and Line File Maintenance

SYS1210 IAFIS (III) shall accept NCIC ORI File Maintenance message in accordance with the III Operation and Technical Manual.

SYS1211 IAFIS (III) shall update the NCIC ORI File using the data contained within the NCIC ORI File Maintenance message.

The IAFIS NCIC ORI file will be kept in sync with NCIC for message validation purposes.

SYS1212 IAFIS (III) shall accept NCIC Line File Maintenance message in accordance with the III Operation and Technical Manual.

SYS1213 IAFIS (III) shall update the NCIC Line File using the data contained within the NCIC Line File Maintenance message.

The IAFIS NCIC Line file will be kept in sync with NCIC for message validation purposes.

3.8.2.7 IAFIS File Synchronization Process

SYS1214 IAFIS shall provide the procedures and tools to detect inter-segment out of synchronization conditions.

SYS1215 IAFIS shall provide the procedures and tools to maintain data synchronization to keep the replicated data and data links synchronized.

SYS1216 IAFIS shall provide the procedures and tools to correct out of synchronization conditions to keep the replicated data and data links synchronized.

SYS1217 IAFIS shall provide a bitmap process to identify internal or external criminal and civil database synchronization errors by allowing System Administrators to compare bitmapped lists of the record identifiers (FNU or CRN) currently active in each segment.

SYS1218 IAFIS (ITN) shall provide the capability to provide a bitmap representation for the active subjects in the FIMF.

SYS1219 IAFIS (ITN) shall provide the capability to provide a bitmap representation for the active subjects in the Civil On-line File.

SYS1220 IAFIS (AFIS) shall provide the capability to provide a bitmap representation for the active subjects in the CMF.

SYS1221 IAFIS (AFIS) shall provide the capability to provide a bitmap representation for the active subjects in the Civil Feature File.

SYS1222 IAFIS (III) shall provide the capability to provide a bitmap representation for the active subjects in the Criminal History File.

SYS1223 IAFIS (III) shall provide the capability to provide a bitmap representation for the active subjects in the Civil History File.

SYS1224 IAFIS shall provide the capability to compare bitmap files from all segments.

3.8.3 System Status and Performance

The System Status and Reporting (SSR) capability provides status information on current response time performance, resources allocated to each environment (e.g., operational, testing), the readiness and availability of hardware components, staffing resources, and other information to identify processing bottlenecks and tune system performance.

SYS1225 IAFIS shall provide the capability for a System Administrator to monitor and manage all inter-segment communications.

SYS1226 IAFIS shall provide the capability for a System Administrator to monitor and manage the status of all external communications.

SYS1227 IAFIS (EFCON) shall provide the capability for authorized operators to monitor the operational status of EFCON from a console.

SYS1228 IAFIS (EFCON) shall provide the capability for a System Administrator to monitor the status of each CJIS WAN submission.

SYS1229 IAFIS (EFCON) shall monitor system transactions from transaction receipt through response transmission.

SYS1230 IAFIS (EFCON) shall provide a real-time graphical interface to monitor and display the current status of the system.

SYS1231 IAFIS (EFCON) shall provide a real-time graphical interface to monitor and display the number of elements in any queue, and the average delay for both queued and non-queued transactions.

SYS1232 IAFIS (EFCON) shall provide a real-time graphical interface to monitor and display averages over the last hour, which is recalculated at a configurable interval (e.g., every two minutes).

SYS1233 IAFIS shall allow Authorized FBI System Administrators access to system status and reporting capabilities.

SYS1234 IAFIS shall collect system status information (i.e., readiness, utilization, queue status) for all system components.

SYS1235 IAFIS shall collect system performance information (i.e., response times, workload).

SYS1236 IAFIS shall allow a System Administrator to view system status information on each active system environment (i.e., operational, development support, and test support).

SYS1237 IAFIS shall allow a System Administrator to view system performance information on each active system environment (i.e., operational, development support, and test support).

SYS1238 IAFIS shall retain historical system status information.

SYS1239 IAFIS shall retain historical system performance information.

NGI-396

Status and performance information for each segment will include current response time performance, resources allocated to each environment, readiness and availability of hardware components, and information that identifies processing bottlenecks and for tuning segment performance.

SYS1240 IAFIS shall allow System Administrators to define system faults for which they should be notified.

SYS1241 IAFIS (ITN) shall provide on-line monitoring and analysis of system performance.

SYS1242 IAFIS (ITN) shall provide threshold alerting capabilities to include but not be limited to the following: response time performance, resources utilized by each environment, readiness and availability of system components, and out of service components.

SYS1243 IAFIS shall notify a System Administrator when a pre-defined system fault occurs.

SYS1244 IAFIS (AFIS) shall notify a System Administrator within two (2) minutes of a deviation in performance from specified standards.

SYS1245 IAFIS shall record software exceptions into a software alert log.

SYS1246 IAFIS shall allow a System Administrator to view the software alert log.

SYS1247 IAFIS shall provide self-test capability for all on-line equipment.

SYS1248 IAFIS (ITN) shall provide off-line diagnostic tools that identify equipment failure modes to Lowest Replaceable Unit (LRU) level to support availability and Maximum Downtime (MDT) requirements.

SYS1249 IAFIS (III) shall provide periodic self-test of on-line major components.

SYS1250 IAFIS (ITN) shall provide segment status information and performance data for each environment.

Segment status information and performance data will include, but not be limited to: threshold alerting, response time performance, resource utilization, readiness and availability of system components, queue depth, and out of service components.

SYS1251 IAFIS (ITN) shall provide routine reports regarding daily, weekly, monthly, and long term performance trends.

SYS1252 IAFIS (III) shall provide segment status information and performance data for each environment.

SYS1253 IAFIS (AFIS) shall provide segment status information and performance data for each environment.

SYS1254 IAFIS (AFIS) shall provide the capability for AFIS System Administrator(s) to select automatic collection and analysis options for operations data, from a menu.

SYS1255 IAFIS (AFIS) shall provide the capability for AFIS System Administrator(s) to select ad hoc data collection and analysis options from a menu, for operations data.

SYS1256 IAFIS (AFIS) shall provide the capability to collect automatic operations data in sufficient quantity and resolution to be able to track and monitor the performance of the AFIS hardware and software components to determine daily, weekly, monthly, and long-term performance trends.

NGI-397

SYS1257 IAFIS shall provide the capability to report a segment outage to the System Administrator(s).

SYS2225 IAFIS (iDSM) shall support automated scripts that daily check the availability of shared data processing servers.

SYS2226 IAFIS (iDSM) shall provide visual alarms to inform system operators or administrators of selected events or violations from the set of system parameters.

3.8.4 Business Rules and Thresholds

SYS1258 IAFIS (ITN) shall maintain business rules to support the Automated Quality Check (AQC) of textual data as part of a Ten-Print Fingerprint Identification Search.

SYS1259 IAFIS (AFIS) shall maintain a configurable parameter for the Automated Sequence Check (ASC) score threshold.

SYS1260 IAFIS (III) shall maintain a configurable parameter for the Subject Search match score threshold.

SYS1261 IAFIS (III) shall maintain a configurable parameter for the Ten-Print Subject Search candidate limit.

SYS1262 IAFIS (III) shall maintain a configurable parameter for the document processing Subject Search candidate limit.

SYS1263 IAFIS (III) shall maintain a configurable parameter for the III/NFF Subject Search candidate limit.

SYS1264 IAFIS (III) shall double the document processing candidate limit for subject search requests from the Service Desk.

SYS1265 IAFIS (III) shall maintain a configurable parameter for the civil subject search candidate limit.

SYS1266 IAFIS (III) shall maintain a configurable parameter for the criminal ad hoc subject search candidate limit.

SYS1267 IAFIS (III) shall maintain a configurable parameter for the civil ad hoc subject search candidate limit.

SYS1268 IAFIS (AFIS) shall maintain a configurable parameter for the fingerprint match threshold.

SYS1269 IAFIS (AFIS) shall maintain a configurable parameter for the Ten-print fingerprint feature search high confidence threshold.

This threshold provides decision point for automated or "lights-out" identification decisions.

SYS1270 IAFIS (AFIS) shall maintain a configurable parameter for the Ten-Print fingerprint feature search low confidence threshold.

This threshold provides decision point as to whether one or two manual FICs are required.

SYS2227 IAFIS (iDSM) shall provide the capability to maintain a shared data high confidence threshold to support automated comparison processes against candidates identified in a shared

data search.

This threshold provides decision point for automated or "lights-out" identification or verification decisions. Maintenance of Shared Data business rules and thresholds allows for the modification of these parameters without impacting iDSM availability.

SYS2228 IAFIS (iDSM) shall provide the capability to maintain a shared data low confidence threshold to support the automated identification processes against candidates identified in a shared data search.

This threshold provides the decision point as to whether one or two iDSM manual image comparisons are required.

SYS1271 IAFIS (ITN/TPS) shall maintain a configurable parameter for the EVAL threshold.

This threshold will allow for additional review by an EVAL Service Provider.

SYS1272 IAFIS (AFIS) shall maintain a configurable parameter for the Latent Fingerprint Feature Search match score threshold.

SYS1273 IAFIS (AFIS) shall maintain a configurable parameter for the Latent Fingerprint Feature Search candidate limit.

SYS1274 IAFIS (AFIS) shall maintain a configurable parameter for the ten-print identification search candidate limit.

SYS1275 IAFIS (AFIS) shall maintain a configurable parameter for the ten-print investigation search candidate limit.

SYS1276 IAFIS (AFIS) shall maintain a configurable parameter for the maximum latent search penetration for each repository.

SYS1277 IAFIS (AFIS) shall provide the capability to maintain a configurable parameter for the maximum latent search penetration for an Authorized Contributor.

SYS1278 IAFIS (AFIS) shall maintain a configurable parameter for the Search but Don't Add (SBDA) fingerprint quality threshold.

SYS1279 IAFIS (AFIS) shall maintain a configurable parameter for fingerprint image quality reject threshold.

SYS1280 IAFIS shall provide the ability to maintain time-out clocks for system, inter-segment, and intra-segment transactions as services are requested and provided in accordance with the IAFIS ICD.

SYS2229 IAFIS shall provide the capability to maintain a daily IAQ search limit.

3.8.5 Transaction History

SYS1281 IAFIS (IDWH) shall maintain a system transaction status file on all system transactions which are currently being processed.

SYS1282 IAFIS (ITN) shall collect near real-time inter-segment status and tracking data for transactions in progress.

SYS1283 IAFIS shall collect status and tracking data for transactions processed by EFCON.

Mar 39

SYS1284 IAFIS shall collect status and tracking data for transactions processed by ITN.

SYS1285 IAFIS shall collect status and tracking data for transactions processed by III.

SYS1286 IAFIS shall collect status and tracking data for transactions processed by AFIS.

SYS2230 IAFIS shall collect status and tracking data for transactions processed by iDSM.

SYS1287 IAFIS shall collect status information that indicates when a system transaction was received.

SYS1288 IAFIS shall collect status information that indicates whether a system transaction was accepted or rejected.

SYS1289 IAFIS shall collect status information that indicates the reason a system transaction rejected.

SYS1290 IAFIS (ITN) shall collect status information that indicates the response due time for a system transaction.

SYS1291 IAFIS shall collect status information that indicates the time and date a response to a system transaction was sent.

SYS1292 IAFIS shall collect status information that indicates the recipient of a response to a system transaction.

IAFIS will also collect the IAFIS Control Number (ICN), the Transaction Control Number (TCN), and FBI Number.

SYS1293 IAFIS shall provide the capability for a System Administrator to perform a transaction status search.

SYS1294 IAFIS (ITN) shall provide the capability for an Authorized FBI Service Provider to perform a transaction status search.

IAFIS will perform a system transaction status search using, but not limited to, any or all of the following transaction status data; ICN, TCN, Transaction Status, Disposition, Function(s) Name and Type, EID, Subject Name, STOT, TSR, RFP, ORI, OAN, CIDN, OCA, FBI Number, and the date/start time and date/completion times for the functions and the submission.

SYS1295 IAFIS shall provide the capability for a System Administrator to view transaction status data.

SYS1296 IAFIS (ITN) shall provide the capability for an Authorized FBI Service Provider to view transaction status data.

A response to a transaction status query may contain the following transaction status data; ICN, TCN, Transaction Status, Disposition, IAFIS Note, Function(s) Name and Type, EID, Modified Data, Subject Name, STOT, TSR, RFP, ORI, OAN, CIDN, OCA, FBI Number, Subject DOB, Subject Social Security Number, and the date/start time and date/completion times for the functions and the submission.

SYS1297 IAFIS shall allow System Administrators to print transaction status data.

SYS1298 IAFIS (ITN) shall allow Authorized FBI Service Providers to print transaction status data.

The history records will be used to perform transaction audits and to generate statistical reports on IAFIS operations. IAFIS will provide access to the history data to authorized operators in order to locate, review, and (if necessary) reproduce the history records for specific transactions.

SYS1299 IAFIS shall collect the history of every user transaction (i.e., submissions, searches, and requests).

SYS1300 IAFIS (ITN) shall allow an Authorized FBI Service Provider to search transaction history data.

SYS1301 IAFIS (ITN) shall allow an Authorized FBI Service Provider to view transaction history data.

SYS1302 IAFIS (ITN) shall allow an Authorized FBI Service Provider to print transaction history data.

SYS1303 IAFIS shall allow a System Administrator to search to transaction history data.

SYS1304 IAFIS shall allow a System Administrator to view transaction history data.

SYS1305 IAFIS shall allow a System Administrator to print transaction history data.

IAFIS (ITN/TPS) will retain the following information in support of transaction history: ICN, TCN (if appropriate), transaction type code, transaction start time, transaction completion time, functions performed (both automated and manual), transaction data modified or added by the function performed, function start times, function completion times, work group that performed each function, work group member that performed each function, input transaction data (minus image data), output transactions data (minus image data) that was added or modified as a result of the function performed, and the ten-print certification file index pointer. IAFIS will store other information in transaction history as necessary.

SYS1306 IAFIS (III) shall record subject and candidate(s) information to support a Subject Search Miss Analysis Tool.

SYS1307 IAFIS shall store transaction history information on-line.

SYS1308 IAFIS shall provide the capability to store transaction history information on off-line media.

SYS1309 IAFIS (IDWH) shall allow an Authorized FBI Service Provider to query the Transaction History data.

IDWH will perform transaction History Searches using the TCN (discrete value and range), IAFIS Control Number (ICN) (discrete value and range), Type of Transaction (TOT) code (up to ten), Function type code (up to ten), ORI (up to ten), FBI Number (up to ten), Date/time range transaction was received, Date/time range transaction completed, Employee Identification Number (EID), and Workgroup identifier.

SYS1310 IAFIS (IDWH) shall allow an Authorized FBI Service Provider to view the Transaction History data.

IDWH will provide the following information in the response from a Transaction History Query: ORI, date/time transaction was received by ITN, date/time transaction completed processing by ITN, code indicating the reason for rejecting the submission, (if any) military code (if applicable), search identification status (non-identification, identification based upon provided

FNU, identification based upon subject/name search, identification based upon fingerprint features search), CRI, TCN, and gender from the Transaction History File.

SYS1311 IAFIS (IDWH) shall allow an Authorized FBI Service Provider to print the Transaction History data.

The following requirements are specific to III Segment Transaction History Reporting:

SYS1312 IAFIS (III) shall provide a III audit function to enable authorized operators to locate, review, and reproduce transactions stored in the III Transaction History File.

SYS1313 IAFIS (III) shall transfer III Transaction History Data to ITN in accordance with the IAFIS ICD.

SYS1314 IAFIS (III) shall provide one day's worth of III Transaction History Data to ITN in each transmission.

One day's worth of Transaction History Data is defined as the data pertaining to all III-owned transactions completed by III during a 24 hour period.

The following requirements are specific to AFIS Segment Transaction History Reporting:

SYS1315 IAFIS (AFIS) shall provide the capability to record all AFIS system and inter-segment transactions, as well as pertinent AFIS intra-segment transactions.

SYS1316 IAFIS (AFIS) shall provide the capability to export selected AFIS operational data.

SYS1317 IAFIS (AFIS) shall provide the capability to maintain pertinent AFIS performance information, operator actions, analyses, and maintenance data for a minimum of seven years.

SYS1318 IAFIS (AFIS) shall provide a transaction log that contains AFIS information for the transaction, the transaction identifier and the date and time of the logged transaction.

SYS1319 IAFIS (AFIS) shall provide the capability for an authorized system administrator to retrieve AFIS operational data.

SYS1320 IAFIS (AFIS) shall provide the capability for an authorized system administrator to generate a hard-copy report of AFIS operational data.

SYS1321 IAFIS (AFIS) shall provide the capability to store the History File for each AFIS transaction on line for 30 calendar days.

SYS1322 IAFIS (AFIS) shall provide the capability to store, after 30 calendar days, the AFIS History File off line on removable media.

SYS1323 IAFIS (AFIS) shall support an expected shelf life of at least 10 years for the off line AFIS History File storage.

SYS1324 IAFIS (AFIS) shall provide the capability to notify the originator of an AFIS Transaction History query when the size of the query response exceeds an operator defined threshold.

SYS1325 IAFIS (AFIS) shall provide a default range limit of 100 transactions or processes when no operator defined threshold is specified in an AFIS Transaction History query.

SYS1326 IAFIS (AFIS) shall provide the capability to support AFIS Transaction History queries against the results of prior queries.

NGI-402

SYS1327 IAFIS (AFIS) shall provide the capability to automatically generate AFIS history reports during periods defined by authorized operators.

SYS1328 IAFIS (AFIS) shall provide the capability to format AFIS history data for presentation in predefined or ad hoc formats.

SYS1329 IAFIS (AFIS) shall provide the capability to support hardcopy and softcopy report generation options for an AFIS history data query.

SYS1330 IAFIS (AFIS) shall provide the capability to support softcopy report file requests in ASCII format for an AFIS history data query.

SYS1331 IAFIS (AFIS) shall provide the capability to transfer softcopy AFIS transaction history report files to removable magnetic media.

SYS1332 IAFIS (AFIS) shall provide the capability to support summarization of AFIS history analysis data for inclusion in AFIS history analysis reports.

SYS1333 IAFIS (AFIS) shall provide the capability to store Transaction History Data of system and inter-segment transactions owned by AFIS (i.e., remote ten-print searches, remote latent searches, unsolved latent searches, and unsolved latent repository maintenance request from users) in the AFIS History File.

SYS1334 IAFIS (AFIS) shall store the following information in the AFIS Transaction History Data File: System Type of Transaction (STOT), IAFIS Control Number (ICN), Originating Agency Identifier (ORI), Date and time transaction submittal to AFIS, Date and time transaction completed by AFIS, Transaction rejection or error code, if any, from output transaction data, Controlling Agency Identifier (CRI) from Input transaction data (if applicable), Number of candidates produced by search, if any, from output transaction data, Transaction Control Number (TCN) (if applicable), and AFIS Segment Control Number (SCNA) (if applicable).

SYS1335 IAFIS (AFIS) shall provide the capability to support queries against the on line and off line AFIS Transaction History File using the following parameters: TCN (discrete value and range), ICN (discrete value and range), Type of Transaction (up to 10), Originating agency identifier (ORI) (up to 10), Date and time of submittal (discrete values and range), and Date and time of completion (discrete values and range).

The following requirements are specific to iDSM Segment Transaction History Reporting:

SYS2231 IAFIS (iDSM) shall record all activity that occurs against the IAFIS Shared Want File as a result of IAFIS data extracts and data analysis.

SYS2232 IAFIS (iDSM) shall record the additions to the Shared Want Image File (SWIF) and Shared Want Directory (SWD) resulting from IAFIS enrollment requests.

SYS2233 IAFIS (iDSM) shall record the demotions resulting from IAFIS demotion requests.

SYS2234 IAFIS (iDSM) shall record the removals resulting from IAFIS removal requests.

SYS2235 IAFIS (iDSM) shall record each activity that is attempted but fails.

SYS2236 IAFIS (iDSM) shall retain the log entries on-line for a minimum of three years to be available for FBI auditors. NGI-403

SYS2237 IAFIS (iDSM) shall record each action (addition, demotion, removal) taken for an FNU.

SYS2238 IAFIS (iDSM) shall capture the file affected (i.e., Shared Want Image File or Shared Want List) per action logged.

SYS2239 IAFIS (iDSM) shall capture the date/time file action initiated per action logged.

SYS2240 IAFIS (iDSM) shall capture the date/time file action completed per action logged.

SYS2241 IAFIS (iDSM) shall provide a function to log activities related to manual image comaparisons.

SYS2242 IAFIS (iDSM) shall provide the following minimum data associated with manual image comparison work performed: Transaction Number, Action, EID, Status, Subject Num (FNU/CRN), Shared List Agency Number, Action Time.

3.8.5.1 Statistical reporting

SYS1336 IAFIS shall provide the capability to generate statistical reports based on transaction history data.

SYS1337 IAFIS (EFCON) shall identify areas in which transactions are not compliant and create agency non-compliance reports when requested.

SYS1338 IAFIS (EFCON) shall produce a daily report of ten-print transaction activity for each contributor that indicates their level of EFTS compliance.

SYS1339 IAFIS (EFCON) shall e-mail agency non-compliance reports to designated submitting agencies when requested.

SYS1340 IAFIS (EFCON) shall provide an interface for the operations data function that does not require knowledge of statistical computation or programming.

SYS1341 IAFIS (EFCON) shall provide for operator definition, storage, retrieval, and modification of multiple data item sets.

SYS1342 IAFIS (EFCON) shall provide the capability to include each data item in a data item set definition.

SYS1343 IAFIS (EFCON) shall provide the capability to include each data item in multiple data item sets simultaneously.

SYS1344 IAFIS (EFCON) shall provide the capability for an operator to define data item set collection start and stop times for all data item sets.

SYS1345 IAFIS (EFCON) shall support definition of data item set start and stop times by either time and date (e.g., 0100, 1 February 1996) or by a data item event (e.g., receipt of a message from the CSAs).

SYS1346 IAFIS (EFCON) shall provide the capability for an operator to define data item set collection intervals to include seconds, minutes, hours, or days.

SYS1347 IAFIS (EFCON) shall provide the capability for an operator to collect the value of

selected data item sets at periodic intervals.

SYS1348 IAFIS (EFCON) shall provide the capability for an operator to report running totals of collected data item sets, or incremental totals during the collection period.

SYS1349 IAFIS (EFCON) shall provide the capability for authorized System Administrators to retrieve, store, modify, and automatically initiate EFCON operations data reports.

SYS1350 IAFIS (EFCON) shall create, maintain, and store formatted reports.

SYS1351 IAFIS (EFCON) shall format the statistical information for presentation in ad hoc formats.

Communications traffic includes packets, files, messages, and IAFIS system transactions. All references to packets include Transport, Network, Data Link, and Physical layer protocol data units.

SYS1352 IAFIS (EFCON) shall provide operational data collection, generation, and reporting of communications traffic to an Authorized System Administrator when requested.

SYS1353 IAFIS (EFCON) shall provide the capability for an Authorized System Administrator to designate operational data collection by communications traffic source, type, or destination, or by any combination thereof.

SYS1354 IAFIS (EFCON) shall provide sufficient data items (with sufficient accuracy) to an Authorized System Administrator when requested and confirm operation in compliance with all EFCON performance requirements.

SYS1355 IAFIS (EFCON) shall collect and report line and link quality to an Authorized System Administrator when requested.

Line and link quality data includes line faults, packets with uncorrectable input errors and uncorrectable output errors, packet delays, average and maximum times, and line utilization by packet count.

SYS1356 IAFIS (EFCON) shall collect and report transport performance to an Authorized System Administrator when requested.

Transport performance data includes connection attempts refused, lost connections, packet retransmissions, and average, variance, and maximum packet size.

SYS1357 IAFIS (EFCON) shall collect and report electronic mail performance to an Authorized System Administrator when requested.

Electronic performance data includes messages transferred, received and sent, message transfers aborted, received and sent, message size (bytes), and average, variance, and maximum message size.

SYS1358 IAFIS (EFCON) shall collect and report transaction traffic to an Authorized System Administrator when requested.

Transaction traffic data includes system transactions received by ORI and Transaction Type, queue sizes, by segment, average, variance, and maximum, system transactions processed by segment, and the average, variance, and maximum system transaction processing times by segment.

SYS1359 IAFIS (EFCON) shall collect and report resource utilization operations data to an Authorized System Administrator when requested.

Collection and reporting interval for resource utilization operations data is a modifiable parameter ranging from one day to one month.

NGI-405

SYS1360 IAFIS (EFCON) shall retain operations data on-line to an Authorized System

Administrator when requested.

The retention period for on-line operations data is a modifiable parameter ranging from one day to one month.

SYS1361 IAFIS (ITN/ISRE) shall maintain operations data on the additions, retrievals, updates, and deletions of image records.

Operations data collected by ITN/ISRE includes the following:

- update operations data
- deletion operations data
- retrieval operations data
- performance operations data
- failure operations data

SYS1362 IAFIS (ITN/ISRE) shall provide cumulative (all files) and individual (each file) operations data for each measurement.

SYS1363 IAFIS (ITN/ISRE) shall provide the capability for authorized operators to retrieve and store ITN/ISRE operations data.

SYS1364 IAFIS (AFIS) shall count high penetration searches as one search for the purposes of latent search processing and accounting.

High penetration searches are those latent searches that exceed the population cap (default is set at 30 percent).

SYS1365 IAFIS (AFIS) shall provide the capability to receive a Latent Repository Statistics Query which contains the requestor's ORI.

SYS1366 IAFIS (AFIS) shall provide the capability to generate a Latent Repository Statistics Report for valid requestors upon receipt of a Latent Repository Statistics Query in accordance with the IAFIS ICD.

SYS1367 IAFIS (AFIS) shall provide the capability for the Latent Repository Statistics Report to include the current repository statistics required to estimate repository penetration.

SYS1368 IAFIS (AFIS) shall provide a monthly report of latent search performance summary upon request by a Latent Specialists.

SYS1369 IAFIS (AFIS) shall provide a monthly report of latent search performance summary upon request by an AFIS administrator.

SYS1370 IAFIS (AFIS) shall provide the capability to collect, record, and analyze information relating to the processing of latent searches.

SYS1371 IAFIS (AFIS) shall provide the capability to perform Latent Workload Accounting at the end of the accounting period.

SYS1372 IAFIS (AFIS) shall provide the capability to generate a Latent Workload Accounting Report to the Segment Administrator within two hours of the close of the 24-hour period.

The Latent Workload Accounting Report will consist of: total number of processed searches; number of searches processed for state and federal organizations supported; number of searches

of each priority level processed; number of "high penetration" searches (those exceeding 30 percent penetration); average duration of searches (not counting "in queue" time) processed; duration of longest time for a search from time of entry until processing was initiated (i.e., time in the queue); duration of shortest time for a search from time of entry until processing was initiated (i.e., time in the queue); and the average duration of times for all searches performed from time of entry until processing was initiated.

SYS1373 IAFIS shall provide the capability for reports and logs to include records of segment performance, records of segment component failures, and records of Segment Administrator actions to correct or prevent segment performance degradation.

Provide System Monitoring

SYS1374 IAFIS (ITN/TPS) shall provide the capability for Authorized FBI Service Providers to access real-time management reports to monitor workloads, observe the quality of work being performed, and control the productivity of work groups.

SYS1375 IAFIS (ITN/TPS) shall present the current queue depths, transactions in process, work group configurations, an Authorized FBI Service Provider log-on status, Authorized FBI Service Provider functions, and Authorized FBI Service Provider functions being performed in real-time management report(s).

SYS1376 IAFIS (ITN/TPS) shall present real-time management reports at a system-wide or work group level, based on the authorization of the requesting Authorized FBI Service Provider.

SYS1377 IAFIS (ITN/TPS) shall allow Authorized FBI Service Providers to establish high and low thresholds for the real-time management data being collected.

SYS1378 IAFIS (ITN/TPS) shall alert Authorized FBI Service Providers when the real-time management report thresholds are exceeded.

SYS2243 IAFIS (iDSM) shall be capable of reporting the number of positive identifications resulting from searches against the IAFIS shared data.

SYS2244 IAFIS (iDSM) shall be capable of reporting the number of positive identifications resulting from searches against the IDENT shared data.

SYS2245 IAFIS (iDSM) shall be capable of reporting the number of fingerprint searches performed against the records contained in the IAFIS shared data.

SYS2246 IAFIS (iDSM) shall be capable of reporting the number of fingerprint searches performed against the records contained in the IDENT shared data.

3.8.5.2 TRT Log

SYS1379 IAFIS (III) shall record, into a TRT log, the FNU of each subject criminal record that is associated with any IAFIS transaction.

SYS1380 IAFIS (III) shall make the TRT log available to the FBI Special Functions systems for read and delete purposes.

3.8.6 Repository Management

NGI-407

SYS1381 IAFIS shall provide file management capabilities to support the creation of logically

separate repositories.

Ten-Print Certification File (TPCF)

SYS1382 IAFIS (ITN) shall provide a Ten-Print Certification File.

SYS1383 IAFIS (ITN) shall maintain the TPCF records that contain an ICN, the subject's FBI Number, the original images of both sides of the fingerprint card, and the rolled and plain impression fingerprint images.

Fingerprint Image Master File (FIMF)

SYS1384 IAFIS (ITN/ISRE) shall provide a Criminal Ten-Print Fingerprint Image Master File.

SYS1385 IAFIS (ITN/ISRE) shall maintain FIMF records that contain up to ten rolled fingerprint image fields corresponding to the ten fingers from a subject's left and right hands.

SYS1386 IAFIS (ITN/ISRE) shall maintain FIMF records that contain up to two four-finger image fields corresponding to the flat impressions of the forefinger, middle finger, ring finger, and little finger of a subject's left and right hands.

SYS1387 IAFIS (ITN/ISRE) shall maintain FIMF records that contain up to two thumb image fields corresponding to the flat thumb impressions from a subject's left and right hands.

SYS1388 IAFIS (ITN/ISRE) shall maintain FIMF records that contain a text data field containing the subject's FBI Number and an ICN.

Criminal Master Features File (CMF)

SYS1389 IAFIS (AFIS) shall provide a Criminal Ten-Print Fingerprint Features Master File (CMF).

SYS1390 IAFIS (AFIS) shall maintain CMF records that contain the fingerprint features for all ten fingers for each subject in the Criminal Ten-Print Fingerprint Image Master File (FIMF).

SYS1391 IAFIS (AFIS) shall maintain a composite criminal ten-print fingerprint feature record in the Criminal Master Features File (CMF).

Subject Criminal History Files

SYS1392 IAFIS (III) shall provide a Subject Criminal History File.

SYS1393 IAFIS (III) shall maintain Subject Criminal History File records that contain each subject's criminal history along with all of the subject's descriptive information and identifying numbers.

SYS1394 IAFIS (III) shall be able to trace specific criminal history information back to the original source document, an image of the source document, or appropriate system transactions.

Civil On-Line Feature File

SYS1395 IAFIS (AFIS) shall maintain Civil Ten-print On-line Feature File records that contain the fingerprint features for all ten fingers for each subject in the Civil On-line Image File.

Civil On-Line Image File

SYS1396 IAFIS (ITN/ISRE) shall provide Civil Ten-print On-line Image File.

SYS1397 IAFIS (ITN/ISRE) shall maintain the Civil Ten-print On-line Image File records that contain up to ten rolled fingerprint image fields corresponding to the ten fingers from a subject's

left and right hands.

SYS1398 IAFIS (ITN/ISRE) shall maintain the Civil Ten-print On-line Image File records that contain up to two four-finger image fields corresponding to the flat impressions of the forefinger, middle finger, ring finger, and little finger of a subject's left and right hands.

SYS1399 IAFIS (ITN/ISRE) shall maintain the Civil Ten-print On-line Image File records that contain up to two thumb image fields corresponding to the flat thumb impressions from a subject's left and right hands.

SYS1400 IAFIS (ITN/ISRE) shall maintain the Civil Ten-print On-line Image File records that contain text data fields containing the subject's unique number (CRN).

Civil Subject Index Master File

SYS1401 IAFIS (III) shall provide a Civil Subject Index Master File.

SYS1402 IAFIS (III) shall maintain the Civil Subject Index Master File records that contain physical and biographical identifiers for each civil subject.

Unsolved Latent Fingerprint File

The Unsolved Latent Fingerprint Image File will be divided into two sub-files, the State and Local (S&L) Sub-file and the Federal Sub-file. In addition, the Federal Sub-file will be further divided into two subsets, the FBI Subset (used by the LFPS) and Other Federal Agencies Subset. AFIS will manage the number of records in the sub-files and subsets.

SYS1403 IAFIS (ITN/ISRE) shall provide an Unsolved Latent Fingerprint Image File (ULF).

SYS1404 IAFIS (ITN/ISRE) shall maintain the ULF records that contain a single fingerprint image.

SYS1405 IAFIS (ITN/ISRE) shall maintain ULF records with text data fields containing the date created, the ICN, and the AFIS Segment Control Number (SCNA).

SYS1406 IAFIS (AFIS) shall maintain Unsolved Latent Fingerprint Feature records that contain the fingerprint features for each image in the ULF.

AFIS will store the following ULF record information; the record identifier, the Controlling Agency Identifier (CRI), identification of the record as temporary or permanent, the finger position, pattern classification, gender, race, height (with range), weight (with range), age (with range), hair color, eye color, scars, marks, and tattoos, arrest numeric code or literal, place of birth, and state of arrest.

Latent Image File (LIF)

The images contained in the Latent Image File could be scanned fingerprints, palm prints, or photos from the crime scene.

SYS1407 IAFIS (ITN/ISRE) shall provide a Latent Image File (LIF).

SYS1408 IAFIS (ITN/ISRE) shall maintain LIF records with one image field.

SYS1409 IAFIS (ITN/ISRE) shall maintain LIF records with text data fields containing the date created, the latent case number, the case extension number, the image designation ID, and originator ID.

Major Case Print File (MCP)

SYS1410 IAFIS (ITN/ISRE) shall provide a Major Case Print File (MCP).

SYS1411 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain up to ten rolled fingerprint image fields corresponding to the ten fingers from a subject's left and right hands.

SYS1412 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain up to two four-finger image fields corresponding to the flat impressions of the forefinger, middle finger, ring finger, and little finger of a subject's left and right hands.

SYS1413 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain up to two thumb image fields corresponding to the flat thumb impressions from a subject's left and right hands.

SYS1414 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain one palm print image containing the image of the left and right palms.

SYS1415 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain one left hand friction ridge image containing the image of the friction ridge impressions of the left hand.

SYS1416 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain one right hand friction ridge image containing the image of the friction ridge impressions of the right hand.

SYS1417 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain one additional information image containing the image of selected impressions as provided by the FBI field office.

SYS1418 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain one text data field containing the subject's FBI Number, year of birth, fingerprint classifications, and date stored.

SYS1419 IAFIS (ITN/ISRE) shall maintain the MCP record that may contain an FBI Number or other unique identifier.

Special Latent Cognizant File

The Special Latent Cognizant Repository is sub-divided into different sub-files or categories. Each sub-file can be owned by either Authorized FBI Service Providers or OFOs and access to the data in these files will be governed by the IAFIS Authorization and Access Rules.

SYS1420 IAFIS (ITN/ISRE) shall provide a Special Latent Cognizant File repository.

SYS1421 IAFIS (ITN/ISRE) shall maintain SLC Fingerprint Image File records that may contain up to ten rolled fingerprint image fields corresponding to the ten fingers from a subject's left and right hands.

SYS1422 IAFIS (ITN/ISRE) shall maintain SLC Fingerprint Image File records that may contain up to two four-finger, image fields corresponding to the flat impressions of the forefinger, middle finger, ring finger, and little finger of a subject's left and right hands.

SYS1423 IAFIS (ITN/ISRE) shall maintain SLC Fingerprint Image File records that may contain up to two thumbs, image fields corresponding to the flat thumb impressions from a subject's left and right hands.

SYS1424 IAFIS (AFIS) shall maintain SLC Feature records that contain the fingerprint features for each image in the SLC.

SYS1425 IAFIS (ITN/ISRE) shall maintain SLC Fingerprint Image File records that may contain images of the textual portions of the ten-print fingerprint card.

SYS1426 IAFIS (ITN/ISRE) shall provide a SLC text file for owners to maintain descriptive

data detailing contents of their SLC sub-file.

ITN/ISRE will store text information for each SLC record in the SLC Text Files, to include subject's record identifier (FBI Number, Civil record number, miscellaneous identification number or unique SLC identifier), year of birth, fingerprint classification, latent case number and image ID as appropriate, date and time of entry, comment field, and reference to associated records in SLC fingerprint mage file.

SYS1427 IAFIS (ITN/ISRE) shall assign and store a unique special file number for each SLC sub-file.

SYS1428 IAFIS (ITN/ISRE) shall assign and store a unique special record file number for each record in a SLC sub-file.

SYS1429 IAFIS (ITN/LPS) shall provide the capability to create and delete logical SLC image, feature, and text files.

Shared Data Files

SYS2247 IAFIS (iDSM) shall maintain a Shared Want Image File (SWIF) that is supported by IAFIS shared data updates.

SYS2248 IAFIS (iDSM) shall maintain a Shared Want Directory (SWD) that is supported by IAFIS shared data updates.

SYS2249 IAFIS (iDSM) shall maintain a Shared Want Activity Log (SWAL) that is supported by IAFIS shared data updates.

The SWIF, SWD and SWAL will be maintained on the SSC/FBI at the DOJ Rockville, MD facility. Features are extracted by IDENT from the images provided in the Shared Want Image File and maintained in the DHS Shared Want Directory for search by IDENT.

SYS2250 IAFIS (iDSM) shall maintain a Shared Watch Image File that is supported by IDENT shared data updates.

SYS2251 IAFIS (iDSM) shall maintain a Shared Watch Directory that is supported by IDENT shared data updates.

SYS2252 IAFIS (iDSM) shall maintain a Shared Watch Activity Log that is supported by IDENT shared data updates.

Features are extracted from the images provided in the Shared Watch Image File and maintained in the FBI Shared Watch Directory for search by IAFIS. These files will be maintained in the CJIS Data Center at the Clarksburg, WV facility.

IAFIS Repositories

SYS1430 IAFIS shall maintain data repositories stored on multiple segments.

As a result of the data repositories stored on multiple segments, certain data elements will be replicated across the segments as shown in Table 3.8.6-1. Table 3.8.6-1 identifies all of the segments which contain the replicated data.

Table 3.8.6-1 IAFIS Data Replication and Synchronization

Replicated Data	ITN File	NGI File	AFIS File

Replicated Data	ITN File	III File	AFIS File
FBI Number	Criminal Ten-Print Fingerprint Image Master	Subject Criminal History	Criminal Ten-Print Fingerprint Features Master
address pointer and IAFIS Control Number (ICN)	Criminal Ten-Print Certification	Subject Criminal History	
unique record identifier	Special Latent Cognizant Ten-Print Image		Special Latent Cognizant Features
unsolved latent record identifier	Unsolved Latent Fingerprint Image		Unsolved Latent Fingerprint Features
Civil Record Number (CRN)	Civil Ten-Print Image Master	Civil Subject Index Master	Civil Ten-Print Features

Support Data Import/Export

SYS1431 IAFIS shall provide the capability for a System Administrator to extract data from IAFIS in bulk formats.

SYS1432 IAFIS shall provide the capability for a System Administrator to write extracted data to removable media.

SYS1433 IAFIS shall provide the capability for a System Administrator to import data extracted from external systems.

National Archive and Records Administration (NARA)

SYS1434 IAFIS (III) shall support the creation of archival tapes in accordance with the NARA agreement.

SYS1435 IAFIS (III) shall transfer criminal history record information and civil subject record information to the NARA in accordance with established agreements.

3.8.7 Store Demographic Data

All demographic data must be searchable and stored online to provide EFCON administrators the ability to respond to a transaction resubmission request.

SYS1436 IAFIS (EFCON) shall store all demographic data online for each transaction for up to one year.

SYS1437 IAFIS (EFCON) shall store all demographic data online for each response for up to 90 days after IAFIS issues a response.

SYS1438 IAFIS (EFCON) shall provide the capability for an EFCON administrator to search all transaction related online demographic data.

SYS1439 IAFIS (EFCON) shall provide the capability for an EFCON administrator to search all response related online demographic data.

NGI-412

3.8.8 System Administration

SYS1440 IAFIS shall allow authorized system administrators to view any information in the record files necessary to perform the administrators' role.

SYS1441 IAFIS (ITN/TPS) shall display all processing suspensions to authorized FBI Service Providers and operators (e.g., ITN/TPS Team Leaders and Segment Administrators).

SYS1442 IAFIS (ITN/TPS) shall communicate failures which may impact the processing of search requests and results to authorized FBI Service Providers and operators.

SYS2253 IAFIS (iDSM) shall support the centralized control and display of system administration functions.

SYS2254 IAFIS (iDSM) shall report system alarms to a centralized system administration display.

Segment Administration Control

SYS1443 IAFIS shall provide III Segment Administration that is independent of the other IAFIS segments.

SYS1444 IAFIS shall provide ITN Segment Administration that is independent of the other IAFIS segments.

SYS1445 IAFIS shall provide AFIS Segment Administration that is independent of the other IAFIS segments.

SYS1446 IAFIS shall provide EFCON Segment Administration that is independent of the other IAFIS segments.

SYS1447 IAFIS shall provide IDWH Segment Administration that is independent of the other IAFIS segments.

SYS1448 IAFIS shall allow Segment Administration (SA) functions to be accessed by authorized personnel from any IAFIS terminal.

SYS1449 IAFIS shall provide the capability for authorized system administrators to access IAFIS operations data.

Operations data is defined as raw or intermediate input and output data generated by the segment. It is intended for analysis or test purposes. IAFIS will measure and compute operations data for transaction input data, transaction processing data, transaction output data, resource utilization operations data, environment data, search data, performance data, failure data, workgroup operations data, and queue operations data.

SYS1450 IAFIS shall provide the capability for authorized system administrators to enable or disable automatic operations data collection.

SYS1451 IAFIS shall provide operations data analysis tools to an authorized system administrator.

The operations data analysis tools will include parameter estimators, including mean and variance, time series analysis tools, trend analysis tools, including growth rate estimators, general graphing tools, histogram generation tools, and utilization estimators.

SYS1452 IAFIS shall provide the capability for an authorized system administrator to collect

NGI-413

operations data for the hour, day, week, month, operation since a specified date, and operation between two specified dates.

SYS1453 IAFIS shall provide the capability for authorized system administrators to indicate for which devices, functions, and/or processes that ad hoc data collection will be enabled or disabled.

SYS1454 IAFIS shall provide the capability for authorized system administrators to generate historical operations data reports.

SYS1455 IAFIS shall maintain performance operations data on-line for a six month on-line retention period.

SYS1456 IAFIS shall maintain selected performance data (e.g., ITN/TPS reliability data) on-line for a one month on-line retention period.

SYS1457 IAFIS shall maintain failure operations data on-line for a one month on-line retention period.

SYS1458 IAFIS shall maintain work group operations data on-line for a six month on-line retention period.

SYS1459 IAFIS shall maintain queue operations data on-line for a six month on-line retention period.

SYS1460 IAFIS shall maintain resource utilization operations data on-line for a one month on-line retention period.

SYS1461 IAFIS shall maintain communications operations data on-line for a six month on-line retention period.

SYS1462 IAFIS shall maintain search operations data on-line for a six month on-line retention period.

SYS1463 IAFIS shall provide the capability for an authorized system administrator to move operations data information off-line on removable media.

SYS1464 IAFIS shall provide the capability for authorized system administrators to define and modify automatic report generation periods.

SYS1465 IAFIS shall provide the capability for authorized system administrators to define and modify automatic data export periods.

SYS1466 IAFIS shall provide the capabilities for an authorized system administrator to select, monitor, report, and display segment maintenance information, status, and diagnostic information.

SYS1467 IAFIS shall provide a workload status display including the processing queue contents, priority, and type of transaction.

SYS1468 IAFIS shall provide the capability for an authorized system administrator to generate and display selected fields from multiple messages and a mix of message types.

Resource Allocation

SYS1469 IAFIS shall provide the capability for an authorized system administrator to reallocate IAFIS resources.

NGI-414

SYS1470 IAFIS shall provide the capability for an authorized system administrator to

reconfigure IAFIS resources.

SYS1471 IAFIS shall provide the capability for an authorized system administrator to tune resources and adjust performance.

SYS1472 IAFIS shall provide the capability for an authorized system administrator to adjust parameters (e.g., search selectivity) to enhance performance.

System Administration Functions

SYS1473 IAFIS shall provide the capability for the system administrator to adjust all IAFIS configurable parameters.

SYS1474 IAFIS shall provide system administration functions with the capability to modify the priority for a single transaction.

SYS1475 IAFIS shall provide the capability for an authorized system administrator to cancel system, inter-segment, or intra-segment transactions from IAFIS.

SYS1476 IAFIS shall provide the capability for an authorized system administrator to suspend system, inter-segment, or intra-segment transactions from IAFIS.

SYS1477 IAFIS shall provide the capability for an authorized system administrator to initiate and control the system data backup and restore functions.

SYS1478 IAFIS shall provide the capability for an authorized system administrator to suspend and abort any IAFIS environment (i.e., NOE, OE, SDL).

SYS1479 IAFIS shall provide the capability for an authorized system administrator to install IAFIS software.

Create Off-line Image Copies

SYS1480 IAFIS (ITN/ISRE) shall provide the capability for an authorized system administrator to create off-line image copies of records in compressed format.

Administer Communications Functions

Administration means the ability to read and report the values of the administered data items. This administration capability will include the ability to define, save, modify, and report data items.

SYS1481 IAFIS (EFCON) shall provide the capability for an operator to administer data items relating to EFCON communications.

SYS1482 IAFIS (EFCON) shall provide the capability for an operator to define, save, modify, and report sets of administration commands for later execution.

SYS1483 IAFIS (EFCON) shall provide the capability to schedule automatic execution of administration commands or saved sets of administration commands.

SYS1484 IAFIS (EFCON) shall provide the capability for an operator to group a number of changes into a set to be applied simultaneously to the data used for on-line operations.

The operator may need to add a new transaction type and simultaneously the route that should be used for system transactions of that type.

SYS1485 IAFIS (EFCON) shall provide for the administration of the electronic mail functions as required for proper system operation.

SYS1486 IAFIS (EFCON) shall provide the capability to execute Network Management (NM)

functions (i.e., without shutting down ITN operations) without the loss of any IAFIS system transactions.

SYS1487 IAFIS (EFCON) shall provide the capability for an operator to suspend EFCON processing of single transactions.

Single transaction types, based on a selected field in a transaction (such as ORI or TOT), can be suspended. The term 'suspend EFCON processing' means 'to modify the normal course of EFCON processing', such as to re-direct a transaction to a holding or analysis queue.

SYS1488 IAFIS (EFCON) shall provide the capability for an operator to suspend EFCON processing of selected groups or sets of transactions (i.e., multiple transactions).

SYS1489 IAFIS (EFCON) shall administer configuration management for ITN communications services, including administration of individual components, communication links, local area networks, and wide area networks.

SYS1490 IAFIS (EFCON) shall be capable of administering multiple logical hierarchies of connections for operation and administration purposes.

SYS1491 IAFIS (EFCON) shall provide the capability for an operator to assign attributes to communications equipment and links (physical and logical) representations (i.e., WAN identification information may be assigned to the ITN connection points and to the associated line).

SYS1492 IAFIS (EFCON) shall provide a graphical user interface that allows an operator to display matching transactions and select the appropriate response for that transaction.

SYS1493 IAFIS (EFCON) shall provide a graphical user interface that allows an Authorized System Administrator to display transactions containing data that matches certain input criteria, and to display responses for these transactions.

EFCON does not provide a GUI to display selected transactions types and all possible response types to that transaction type.

SYS1494 IAFIS (EFCON) shall provide a graphical interface that allows an operator to stop and start EFCON as needed.

SYS1495 IAFIS (EFCON) shall provide a graphical interface that allows an operator to stop and start EFCON sub-processes as needed.

SYS1496 IAFIS (EFCON) shall provide a graphical interface that will allow an operator to display transactions that are nearing the IAFIS response time targets, based upon an operator selected time frame.

SYS1497 IAFIS (EFCON) shall provide the capability to perform all Network Management functions through a console.

SYS1498 IAFIS (EFCON) shall provide for authorized operators to access the NM functions.

SYS1499 IAFIS (EFCON) shall provide the capability for operators to initiate printing from their consoles.

SYS1500 IAFIS (EFCON) shall provide the capability for operators to initiate printing of the current screen display.

SYS1501 IAFIS (EFCON) shall provide the capability for operators to save a copy of the current

display for later display.

SYS1502 IAFIS (EFCON) shall provide the capability for an operator to modify IAFIS Time.

SYS1503 IAFIS (EFCON) shall allow for the entry of the time to the nearest 0.05 seconds.

SYS1504 IAFIS (EFCON) shall provide an address translation function for routing system transactions based on transaction type.

SYS1505 IAFIS (EFCON) shall administer all protocol and service operation data items, including addressing and routing tables in all ITN communications services (e.g., electronic mail) and devices (e.g., routers).

SYS1506 IAFIS (EFCON) shall administer IAFIS system transaction formats.

SYS1507 IAFIS (EFCON) shall support multiple valid IAFIS formats.

SYS1508 IAFIS (EFCON) shall identify an IAFIS system transaction format based on system transaction field values.

SYS1509 IAFIS (EFCON) shall administer all system transaction validation parameters.

SYS1510 IAFIS (EFCON) shall provide the capability for an operator to select single or repeated test executions.

SYS1511 IAFIS (EFCON) shall provide the capability for an operator to designate tests to repeat continuously until stopped or for a specified number of repetitions.

SYS1512 IAFIS (EFCON) shall record both intermittent and hard failure incidents from selected tests.

SYS1513 IAFIS (EFCON) shall provide the capability for an operator to select the recording device (e.g., fixed disk, printer, or communications port).

SYS1514 IAFIS (EFCON) shall support data collection, analysis, and reporting of operations data to an EFCON operator.

SYS1515 IAFIS (EFCON) shall provide the capability for an operator, while the system remains on-line, to isolate IAFIS components and groups of components for maintenance and diagnostic purposes.

Provide Startup and Shutdown Commands

SYS1516 IAFIS shall provide the capabilities for authorized system administrators to perform startup commands for each segment which allow for the orderly initialization of the segment operations.

SYS1517 IAFIS shall provide the capabilities for authorized system administrators to perform shutdown commands for each segment which allow for the orderly termination of the segment operations.

Latent System Administrator

This capability will be restricted to authorized LFPS specialists only, who will perform these functions for LFPS and on behalf of OFO.

SYS1518 IAFIS (AFIS) shall provide the capabilities for an authorized system administrator to view the current status of SLC file distribution across processing servers.

NGI-417

SYS1519 IAFIS (AFIS) shall provide capabilities for an authorized system administrator to

create a logical SLC file across processing servers up to the maximum number of SLC records.

SYS1520 IAFIS (AFIS) shall provide the capabilities for an authorized system administrator to modify the allocated size of a SLC up to the maximum number of SLC records.

Each SLC File may be a separate collection of image records or a logical grouping of image records in other ITN/ISRE image files, or some combination of both.

SYS1521 IAFIS (AFIS) shall provide the capabilities for an authorized system administrator to selectively process latent searches that exceed the default parameters.

3.8.9 System Backup and Recovery

SYS1522 IAFIS shall support the creation of backup data for IAFIS repository data.

SYS1523 IAFIS shall support the creation of backup data for IAFIS system files.

SYS1524 IAFIS shall support the creation of backup data for IAFIS application files.

SYS1525 IAFIS shall ensure that IAFIS user services are available during backup operations.

SYS1526 IAFIS shall perform backup routines without interrupting operational processing.

SYS1527 IAFIS shall satisfy all functional and performance requirements while backups are being performed.

SYS1528 IAFIS shall provide the capability to perform back up and maintenance activities with no impact to IAFIS availability.

SYS1529 IAFIS shall provide the capability to restore work in process for each system transaction to its most recently completed step, in the event of system failure.

SYS1530 IAFIS shall support export of backup data to removable media.

The removable backup media will periodically be removed to a government provided off-site storage area.

SYS1531 IAFIS shall provide the capability to perform ITN Backups independent of other IAFIS segments.

SYS1532 IAFIS shall provide the capability to perform ITN/ISRE Backups independent of other IAFIS segments.

SYS1533 IAFIS shall provide the capability to perform III Backups independent of other IAFIS segments.

SYS1534 IAFIS shall provide the capability to perform AFIS Backups independent of other IAFIS segments.

SYS1535 IAFIS shall provide the capability to perform EFCON Backups independent of other IAFIS segments.

SYS1536 IAFIS shall provide the capability to perform IDWH Backups independent of other IAFIS segments.

SYS1537 IAFIS shall provide the capability to perform backups of data stored between specified time periods.

NGI-418

SYS1538 IAFIS shall backup work in process once every 24 hours.

SYS1539 IAFIS shall provide the capability for an authorized system administrator to define the time that backups will begin.

SYS1540 IAFIS shall provide the capability for full or partial backups of maintained data files and application software on removable media.

SYS1541 IAFIS shall be capable of creating incremental backups that contain all IAFIS data which has changed since the time of the most recent backup.

SYS1542 IAFIS (EFCON) shall backup transaction and response information together.

SYS1543 IAFIS (EFCON) shall support the permanent backup of criminal transactions.

SYS1544 IAFIS (EFCON) shall support the temporary backup of civil transactions.

EFCON will permanently erase archival tapes of civil transactions after 90 days.

System and Data Restore

SYS1545 IAFIS shall support the restoration of IAFIS repository data from backup files.

SYS1546 IAFIS shall support the restoration of IAFIS system files from backup files.

SYS1547 IAFIS shall support the restoration of IAFIS application files from backup files.

SYS1548 IAFIS shall provide the capability to perform ITN File Restorations independent of other IAFIS segments.

SYS1549 IAFIS shall provide the capability to perform ITN/ISRE File Restorations independent of other IAFIS segments.

SYS1550 IAFIS shall provide the capability to perform III File Restorations independent of other IAFIS segments.

SYS1551 IAFIS shall provide the capability to perform AFIS File Restorations independent of other IAFIS segments.

SYS1552 IAFIS shall provide the capability to perform EFCON File Restorations independent of other IAFIS segments.

SYS1553 IAFIS shall provide the capability to perform IDWH File Restorations independent of other IAFIS segments.

SYS1554 IAFIS shall provide the capability to perform file restorations of data stored between specified time periods.

SYS1555 IAFIS shall provide the capability to restore IAFIS data to a point in time.

SYS1556 IAFIS shall provide the capability for full or partial restoration of maintained data files and application software from removable media.

IAFIS will be capable of restoring data based on any one or a combination of complete files, records stored between specified dates and times, subject records, storage device, specified date and time, and specified data sets.

SYS1557 IAFIS shall accept a hardware or software failure without losing a system transaction.

SYS1558 IAFIS shall continue processing system transactions despite the system being unable to satisfy the response time and workload requirements.

NGI-419

SYS1559 IAFIS shall resume processing previously suspended system transactions upon

correction of a system failure.

SYS1560 IAFIS shall maintain segment level functionality when other segments become unavailable.

SYS1561 IAFIS shall provide the capability for a System Administrator to initiate and control system recovery.

SYS1562 IAFIS shall support the capability to reassign work from a failed component to remaining functional components in event of hardware or software failure.

3.8.10 System Training and Analysis Support

3.8.10.1 Fingerprint Search Analysis

SYS1563 IAFIS (AFIS) shall provide authorized FBI System Administrators with throughput analysis tools.

SYS1564 IAFIS (AFIS) shall provide authorized FBI System Administrators with fingerprint matching confidence analysis tools.

SYS1565 IAFIS (AFIS) shall provide authorized FBI System Administrators with fingerprint characteristic quality rating analysis tools.

SYS1566 IAFIS (AFIS) shall provide authorized FBI System Administrators with search reliability analysis tools.

SYS1567 IAFIS (AFIS) shall provide authorized FBI System Administrators with search selectivity analysis tools.

3.8.10.2 Subject Search Research

SYS1568 IAFIS (III) shall provide authorized FBI System Administrators with Subject Search miss analysis tool capabilities.

SYS1569 IAFIS (III) shall provide the capability for the system administrator to research how the final descriptor score was determined to include providing the descriptor match scores for individuals not included in the search candidate list.

SYS1570 IAFIS (III) shall provide a modifiable parameter to indicate whether subject search research data will be collected and saved for QH requests.

SYS1571 IAFIS (III) shall provide a modifiable parameter to indicate whether subject search research data will be collected and saved for subject searches other than QH requests.

SYS1572 IAFIS (III) shall allow the collection and retention of subject search research data for both QH and non-QH subject searches simultaneously.

SYS1573 IAFIS (III) shall provide up to three days' worth of subject search research data on-line.

SYS1574 IAFIS (III) shall provide the capability to retrieve subject search scoring information from a previously run search.

SYS1575 IAFIS (III) shall provide the capability to print the subject search research data.

SYS1576 IAFIS (III) shall provide the capability to retrieve subject search scoring information

by ICN.

3.8.10.3 Service Provider Training

SYS1577 IAFIS (ITN) shall provide a training system environment that allows Authorized FBI Service Providers to perform all of the IAFIS operational functions in the manner in which they shall be performed on the operational IAFIS system.

SYS1578 IAFIS (ITN) shall provide interactive Computer Based Training (CBT) for all Authorized FBI Service Provider functions and activities as part of the non-operational training environment.

SYS1579 IAFIS (ITN) shall provide access to all software-based training programs as part of the non-operational training environment.

SYS1580 IAFIS (ITN) shall provide access for operators, trainers, and Authorized FBI Service Providers to the non-operational training environment.

3.8.10.4 System Administration Training

SYS1581 IAFIS shall provide interactive training for System Administrator functions as part of the non-operational training environment.

SYS1582 IAFIS shall provide the ability to perform System Administrator training on all IAFIS workstations and consoles.

SYS1583 IAFIS shall provide the ability to perform System Administrator training related to the handling of operational failures and operations under varying workloads.

3.8.11 Workstation/HMI Support

3.8.11.1 Support General Processing Workstation

SYS1584 IAFIS (ITN) shall adhere to the current version of the HMI Style Guide for all HMI development.

SYS1585 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to initiate a Criminal History Request and accept its response on an IAFIS workstation.

SYS1586 IAFIS (ITN) shall validate Authorized FBI Service Provider manually entered data according to IAFIS ICD.

SYS1587 IAFIS (ITN) shall generate and display appropriate responses to the Authorized FBI Service Provider to indicate successful manual data entry or data errors.

SYS1588 IAFIS (ITN) shall provide the capability of the IAFIS workstation to initiate fingerprint feature searches against the ten-print data files.

SYS1589 IAFIS (ITN) shall provide the capability of the IAFIS workstation to display magnified fingerprint images.

SYS1590 IAFIS (ITN) shall provide the capability of the IAFIS workstation to enter search parameters.

SYS1591 IAFIS (ITN) shall provide the capability of the IAFIS workstation to review candidate lists and associated fingerprint images.

SYS1592 IAFIS (ITN) shall provide the capability of the IAFIS workstation to display fingerprint images for comparison.

SYS1593 IAFIS (ITN) shall provide the capability of the IAFIS workstation to apply decompression algorithms.

SYS2255 IAFIS (iDSM) shall support shared data terminals or workstations that provide direct access in a controlled environment.

3.8.11.1.1 Provide Local Hardcopy Generation

SYS1594 IAFIS (ITN) shall provide the layout of the printed Fingerprint Image Master File (FIMF) and the Civil Ten-print Master File information to conform to the ten-print card standard to which it applies, as described in the Specification for CJIS Division Fingerprint Cards ten-print card standards for the FD-249 Criminal, FD-258 Applicant, and FD-353 Personal Identification fingerprint cards.

SYS1595 IAFIS (ITN) shall print hardcopy fingerprint image responses with sufficient quality in accordance with the EFTS.

SYS1596 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to print the IAFIS Workstation screen.

SYS1597 IAFIS (ITN) shall provide the capability of the IAFIS workstation to print images.

SYS1598 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to print one fingerprint image.

SYS1599 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to print two side-by-side fingerprint images.

SYS1600 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to print candidate information from a search.

SYS1601 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to print system transaction information.

SYS1602 IAFIS (ITN) shall provide the capability of the IAFIS workstation to meet the print text requirements specified in table 3.8.11-1

Table 3.8.11-1 ITN Printer Requirements

Printer Requirements	Text
Print Density	300 dpi
Pages Per Minute	5
Paper Size	8.5 x 11 inches
Min. Capacity	200 sheets
Max. Type size	32 pts.

SYS1603 IAFIS (ITN) shall provide print queue capabilities on the IAFIS workstation for all ITN printers.

SYS1604 IAFIS (ITN) shall provide the capability for each IAFIS workstation to be assigned a default printer by the Segment Administrator.

SYS1605 IAFIS (ITN) shall provide the capability for the Authorized FBI Service Provider to be able to override the default printer assignment for an individual print request.

3.8.11.1.2 Provide Digital Image Processing Tools

SYS1606 IAFIS (ITN) shall provide the capability of the IAFIS workstation to include a display conforming to the IAFIS image quality specifications contained in the EFTS.

SYS1607 IAFIS (ITN) shall provide the capability of the IAFIS workstation to support digital image processing tools that zoom a displayed image.

SYS1608 IAFIS (ITN) shall provide the capability of the IAFIS workstation to support digital image processing tools that pan (horizontally shift) a displayed image.

SYS1609 IAFIS (ITN) shall provide the capability of the IAFIS workstation to support digital image processing tools that scroll (vertically shift) a displayed image.

SYS1610 IAFIS (ITN) shall provide the capability of the IAFIS workstation to support digital image processing tools that provide brightness controls for a displayed image.

SYS1611 IAFIS (ITN) shall provide the capability of the IAFIS workstation to support digital image processing tools that provide contrast controls for a displayed image.

SYS1612 IAFIS (ITN) shall provide the capability of the IAFIS workstation to support digital image processing tools that mark features for a displayed image.

The effects of manipulation or enhancement will not have any impact on the originally captured image.

3.8.11.1.3 Support Manual Data Entry

SYS1613 IAFIS (ITN) shall provide the capability of the IAFIS workstation to include a keyboard as the standard input device for textual data.

SYS1614 IAFIS (ITN) shall provide the capability of the IAFIS workstation to include a keyboard with a QWERTY layout, at least ten dedicated function keys, dedicated cursor control keys, and a numeric keypad.

SYS1615 IAFIS (ITN) shall provide the capability of the IAFIS workstation to include a secondary input device (e.g., mouse, trackball, special function keyboard, light pen) approved by the FBI.

3.8.11.1.4 Support 508-Compliant Employee Workstations

IAFIS workstations and consoles will have the capabilities described below to ensure that accessibility requirements are met for all current and prospective employees with disabilities.

SYS1616 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to be capable of supporting an alternate keyboard in place of the standard keyboard.

SYS1617 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a keyboard alternative which will execute multiple keystroke commands (e.g., "CTRL-C") serially rather than simultaneously.

SYS1618 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a keyboard alternative which will support disabling and adjustment of the keyboard repeat tolerances.

SYS1619 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a keyboard alternative which will support the emulation of a mouse or similar pointing input

device movements from the keyboard.

SYS1620 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a keyboard alternative which will support visual and auditory indication of key status for the Number Lock, Shift/Caps Lock, and Scroll Lock keys.

SYS1621 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a keyboard alternative which will support the adjustment of volume level of the keyboard audible feedback.

SYS1622 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a keyboard alternative which will provide a physical connection via a physical port (e.g., standard keyboard connection socket, serial, parallel).

SYS1623 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to be capable of supporting a Monitor Enhancement that magnifies text and graphics.

SYS1624 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a Monitor Enhancement with user definable magnification levels from 2 to 8 time's normal output in graduations of 1x.

SYS1625 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a Monitor Enhancement with the ability to toggle the magnification on and off returning the display to normal output.

SYS1626 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a Monitor Enhancement with user definable views (e.g., full screen, partial screen, single line magnification).

SYS1627 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support a Monitor Enhancement with user definable attribute settings (e.g., cursor tracking, highlight identification, color definition, font definition).

SYS1628 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support an IAFIS Enhanced Workstations which will supply an integrated function that provides a visual response to the user to notify the user of significant system activity.

SYS1629 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support an IAFIS Enhanced Workstations which will supply a non-auditory cue or on-screen notification.

SYS1630 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support an IAFIS Enhanced Workstations which will supply equivalent access to the E-Mail system for the hearing and/or speech impaired and mobility-impaired Authorized FBI Service Providers.

SYS1631 IAFIS (ITN) shall provide the capability for the IAFIS Workstations to support an IAFIS Enhanced Workstations which will supply user notification of an incoming or previously received e-mail message by an auditory cue or use of a non-auditory cue.

3.8.11.2 Provide Ten-Print Processing Workstations

SYS1632 IAFIS (ITN) shall support all fingerprint service functions using an IAFIS workstation.

SYS1633 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Providers to manually enter data in support of ten-print processing on a Ten-Print workstation.

SYS1634 IAFIS (ITN/TPS) shall require a forwarding Authorized FBI Service Provider to include reason(s) for forwarding in support of Ten-Print forward processing.

SYS1635 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider who is forwarding a transaction to request a response back indicating how the transaction was resolved.

SYS1636 IAFIS (ITN/TPS) shall use the baseline set of rejection rules in Table 3.8.11-2 to determine if an Authorized FBI Service Provider is authorized to reject transactions.

Table 3.8.11-2 Baseline Rejection Rules

Function	Service Provider Level	Reject	Reject Destination
QC	Level 1	Yes	Message to Contributor
	Level 2	Yes	Message to Contributor
LER	Level 1	Yes	Message to Contributor
	Level 2	Yes	Message to Contributor
EVAL	Level 1	No	—
	Level 2	No	—
	Level 3	Yes	Message to Contributor
	Level 4	Yes	Message to Contributor
FIC	Level 1	No	—
	Level 2	Yes	Message to Contributor
	Level 3	Yes	Message to Contributor
	Level 4	Yes	Message to Contributor
FSC	Level 1	No	—
	Level 2	Yes	Message to Contributor
QA	Level 1	No	—

3.8.11.2.1 Support Quality Check

SYS1637 IAFIS (ITN/TPS) shall provide the capability for an authorized FBI Service Providers to review textual electronic ten-print transactions as part of a Quality Check (QC) function on a Ten-Print workstation.

SYS1638 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to forward a transaction to another Authorized FBI Service Provider as part of the QC function on a Ten-Print workstation.

SYS1639 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to reject ten-print transactions as part of the QC function on a Ten-Print workstation.

SYS1640 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to create a rejection message to the user as part of the QC function on a Ten-Print workstation.

SYS1641 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to retrieve and display reference information such as a NCIC criminal code table on a Ten-Print workstation.

SYS1642 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to modify the submission so that it meets acceptable criteria on a Ten-Print workstation.

SYS1643 IAFIS (ITN/TPS) shall provide the next available QC transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider has completed the current transaction on a Ten-Print workstation.

NGI-425

SYS1644 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to exit the QC application upon completion of the current transaction on a Ten-Print workstation.

3.8.11.2.2 Support Manual Fingerprint Sequence Check (FSC)

SYS1645 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to perform a manual fingerprint image sequence check of ten-print transactions on a Ten-Print workstation.

SYS1646 IAFIS (ITN/TPS) shall display fingerprint images for comparison of rolled to plain impressions for manual fingerprint sequence check on a Ten-Print workstation.

SYS1647 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to designate which images to display first when a new transaction is displayed (e.g., view right thumb prints first) to support manual sequence check on a Ten-Print workstation.

SYS1648 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to change the sequence of each rolled fingerprint to support manual fingerprint sequence check on a Ten-Print workstation.

SYS1649 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to change the sequence of plain impressions on a Ten-Print workstation.

SYS1650 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to apply a stamp to an appropriate fingerprint to support manual fingerprint sequence check on a Ten-Print workstation.

The stamp will indicate the presence of a scar or an amputation on a finger, as well as a finger which was unable to be printed (e.g., bandaged), or if the fingerprint was intentionally omitted.

SYS1651 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to forward a transaction to another Service Provider to support manual sequence check on a Ten-Print workstation.

SYS1652 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to confirm any sequence change(s) they made to support manual sequence check on a Ten-Print workstation.

SYS1653 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to view a history of any sequence changes made to the current transaction to support manual sequence check on a Ten-Print workstation.

SYS1654 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to reject the fingerprint images to support manual sequence check on a Ten-Print workstation.

SYS1655 IAFIS (ITN/TPS) shall provide the next available FSC transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider has completed the current FSC transaction on a Ten-Print workstation.

SYS1656 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to exit the FSC application upon completion of the current transaction on a Ten-Print workstation.

3.8.11.2.3 Support Fingerprint Image Comparison (FIC)

SYS1657 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to perform a fingerprint image comparison (FIC) of ten-print transactions on a Ten-Print

workstation.

SYS1658 IAFIS (ITN/TPS) shall present a submission image and a fingerprint candidate image to an Authorized FBI Service Provider in support of FIC on a Ten-Print workstation.

SYS1659 IAFIS (ITN/TPS) shall concurrently display a selected fingerprint from a ten-print submission with the corresponding fingerprint from a candidate when requested by an Authorized FBI Service Provider in support of FIC on a Ten-Print workstation.

SYS1660 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to select the plain impression fingerprints for comparison with corresponding rolled fingerprint images in support of FIC on a Ten-Print workstation.

SYS1661 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provide to indicate a positive identification decision on a candidate in support of FIC on a Ten-Print workstation.

SYS1662 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provide to indicate a non-identification decision on a candidate in support of FIC on a Ten-Print workstation.

SYS1663 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to forward the submission and the candidate to a higher level Service Provider (e.g., Skill Level 2, 3, or 4 Service Provider) if the FIC Service Provider cannot determine the submission decision in support of FIC on a Ten-Print workstation.

SYS1664 IAFIS (ITN/TPS) shall provide the capability for FIC Service Providers to forward transactions to a specific Authorized FBI Service Provider who is authorized to process FIC transactions.

SYS1665 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to replace candidate fingerprint images with submission fingerprint images during a positive identification decision in support of FIC on a Ten-Print workstation.

SYS1666 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to confirm fingerprint image replacement(s) made on the current transaction during a positive identification decision in support of FIC on a Ten-Print workstation.

The fingerprint image replacement request from a Service Provider will be verified before the action is taken.

SYS1667 IAFIS (ITN/TPS) shall provide the next available FIC transaction to the Authorized FBI Service Provide after the Authorized FBI Service Provider completed the current FIC transaction in support of FIC on the Ten-Print workstation.

SYS1668 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to exit the FIC application upon completion of the current transaction on a Ten-Print workstation.

3.8.11.2.4 Support Evaluation for Questionable Verification (EVAL)

SYS1669 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to perform an evaluation review in support of EVAL on a Ten-Print workstation.

SYS1670 IAFIS (ITN/TPS) shall present a submission image and a fingerprint candidate image to an Authorized FBI Service Provider in support of EVAL on a Ten-Print workstation.

SYS1671 IAFIS (ITN/TPS) shall concurrently display a selected fingerprint from a ten-print submission with the corresponding fingerprint from a candidate when requested by an Authorized FBI Service Provider in support of EVAL on a Ten-Print workstation.

SYS1672 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to select the plain impression fingerprints for comparison with corresponding rolled fingerprint images in support of EVAL on a Ten-Print workstation.

SYS1673 IAFIS (ITN/TPS) shall indicate the latest decision made for the current candidate in support of EVAL on a Ten-Print workstation.

SYS1674 IAFIS (ITN/TPS) shall provide the capability for a Service Provide to indicate a positive identification decision on a candidate in support of EVAL on a Ten-Print workstation.

SYS1675 IAFIS (ITN/TPS) shall provide the capability for a Service Provide to indicate a non-identification decision on a candidate in support of EVAL on a Ten-Print workstation.

SYS1676 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to replace candidate fingerprint images with submission fingerprint images during a positive identification decision in support of EVAL on a Ten-Print workstation.

SYS1677 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to confirm fingerprint image replacement(s) made on the current transaction during a positive identification decision in support of EVAL on a Ten-Print workstation.

The fingerprint image replacement request from a Service Provider will be verified before the action is taken.

SYS1678 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to reject an EVAL transaction when reviewing the first candidate of a multi-candidate transaction in support of EVAL on a Ten-Print workstation.

SYS1679 IAFIS (ITN/TPS) shall provide the next candidate image of a multi-candidate transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider has made a decision on the current candidate in support of EVAL on the Ten-Print workstation.

SYS1680 IAFIS (ITN/TPS) shall provide the next available EVAL transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider completed the current EVAL transaction in support of EVAL on the Ten-Print workstation.

SYS1681 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to exit the EVAL application upon completion of the current transaction on a Ten-Print workstation.

3.8.11.2.5 Support Logic Error Resolution (LER)

The Logic Error Resolution (LER) function is used to review error transactions that result from inconsistency between the Subject Criminal History File (SCHF) update and the SCHF. Examples of logic errors are:

a. attempting to add information that exceeds the table storage capacity (e.g., Date of Birth table)

b. attempting to add duplicate information (e.g., an arrest that is already on file)

c. attempting to use submission data that is invalid or inconsistent with SCHF data (e.g., attempting to add an individual with an SID that has been assigned to another individual in

the SCHF)

The category of logic errors that involves exceeding table storage capacity may be repairable through human intervention.

SYS1682 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to perform a logic error review in support of LER on a Ten-Print workstation.

SYS1683 IAFIS (ITN/TPS) shall display the submission, the subject's criminal history record, and the error message(s) in support of LER on a Ten-Print workstation.

SYS1684 IAFIS (ITN/TPS) shall display the error message(s) as described in the IAFIS ICD in support of LER on a Ten-Print workstation.

SYS1685 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to correct the submission data in support of LER on a Ten-Print workstation.

SYS1686 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to correct the criminal history record in support of LER on a Ten-Print workstation.

SYS1687 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to resubmit the update to the criminal history master record in support of LER on the Ten-Print workstation.

SYS1688 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to reject the submission and add explanatory text for the rejection in support of LER on the Ten-Print workstation.

SYS1689 IAFIS (ITN/TPS) shall provide the capability for the Authorized FBI Service Provider to forward the submission to another Authorized FBI Service Provider in support of LER on the Ten-Print workstation.

SYS1690 IAFIS (ITN/TPS) shall provide the next available LER transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider completed the current LER transaction in support of LER on the Ten-Print workstation.

SYS1691 IAFIS (ITN/TPS) shall allow the Authorized FBI Service Provider to exit the LER application upon completion of the current transaction on a Ten-Print workstation.

3.8.11.2.6 Support Transaction Forward Review

The Forward Review (FR) mode will be used by authorized Service Providers to perform a review of data that previously forwarded. During the review period, the normal processing flow for the transaction is interrupted until the review is complete. The mode can be performed on the QC, FSC, FIC, and LER functions.

SYS1692 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to perform transaction review in support of FR mode on the Ten-Print workstation.

SYS1693 IAFIS (ITN/TPS) shall provide the capability for Authorized FBI Service Providers to receive a forwarded transaction from another Service Provider in support of FR mode on the Ten-Print workstation.

SYS1694 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to receive transactions forwarded by Service Providers within the same work group in support of FR mode on the Ten-Print workstation. NGI-429

SYS1695 IAFIS (ITN/TPS) shall provide the next available FR transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider has completed the current FR transaction in support of FR mode on the Ten-Print workstation.

SYS1696 IAFIS (ITN/TPS) shall allow Authorized FBI Service Provider to exit the FR application upon completion of the current transaction in support of FR mode on the Ten-Print workstation.

3.8.11.2.7 Provide Processing Quality Assurance

The Quality Assurance (QA) review mode will be used by authorized Service Providers to perform a review of data. During the review period, the normal processing flow for the transaction is interrupted until the review is complete. The mode can be performed on the FSC and FIC functions.

SYS1697 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to manually review system transaction data in support of QA on a Ten-Print workstation.

SYS1698 IAFIS (ITN/TPS) shall provide the QA Service Provider performing a FSC review with the same functionality as the FSC processing on the Ten-Print workstation.

SYS1699 IAFIS (ITN/TPS) shall provide the QA Service Provider performing a FIC review with the same functionality as the FIC processing on the Ten-Print workstation.

SYS1700 IAFIS (ITN/TPS) shall provide the next available QA transaction to the Authorized FBI Service Provider after the Authorized FBI Service Provider has completed the current QA transaction in support of QA mode on the Ten-Print workstation.

SYS1701 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to exit the QA application upon completion of the current transaction in support of QA mode on the Ten-Print workstation.

3.8.11.2.8 Provide Ten-Print Transaction Review

The Ten-Print Transaction Review (TR) will be used by authorized Service Providers to perform a review of data from an ITN/TPS system transaction that has been handled by a Service Provider which had 'Transaction Review' turned on in their profile. During the review period, the normal processing flow for the transaction is interrupted until the review is complete. This mode can be performed on the QC, FSC, FIC, and LER functions.

SYS1702 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to review ten-print transaction data in support of TR mode on a Ten-Print workstation.

SYS1703 IAFIS (ITN/TPS) shall provide the capability for a reviewing Authorized FBI Service Provider to specify the employee identification number (EID) and function being performed in support of TR mode on a Ten-Print workstation.

SYS1704 IAFIS (ITN/TPS) shall provide the capability for the reviewing Authorized FBI Service Provider to modify the system transaction data as part of the TR function on a Ten-Print workstation.

SYS1705 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to release all data that has been collected for TR onto the next function in support of the TR mode on a Ten-Print workstation.

NGI-430

The process of moving collected TR data onto the next the function is known as the 'TR Flush'. This is an automated function that is triggered by the response from the reviewing Service Provider during the shutdown of the TR application.

SYS1706 IAFIS (ITN/TPS) shall provide the next available TR transaction to the reviewing Authorized FBI Service Provider after the reviewing Authorized FBI Service Provider completed the current TR transaction in support of the TR mode on a Ten-Print workstation.

SYS1707 IAFIS (ITN/TPS) shall allow an Authorized FBI Service Provider to exit the TR application upon completion of the current transaction in support of the TR mode on a Ten-Print workstation.

3.8.11.2.9 Support Post Process Review

This Post Process Review (PPR) occurs after the transaction has completed processing and does not impact the transaction processing flow. The authorized Service Provider will review how the forwarded or rejected transaction was processed and provide off-line feedback to the forwarding or rejecting Service Provider, if necessary.

SYS1708 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to review completed transaction data in support of PPR mode on a Ten-Print workstation.

SYS1709 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to access transactions that were rejected by Authorized FBI Service Providers from the same work group in support of the PPR mode on a Ten-Print workstation.

SYS1710 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to access transactions that were forwarded by Authorized FBI Service Providers from the same work group in support of the PPR mode on a Ten-Print workstation.

SYS1711 IAFIS (ITN/TPS) shall provide the capability for an Authorized FBI Service Provider to access transactions from a specific Authorized FBI Service Provider in support of the PPR mode on a Ten-Print workstation.

SYS1712 IAFIS (ITN/TPS) shall provide the capability for Authorized FBI Service Providers to mark a transaction for deletion after reviewing the transaction in support of the PPR mode on a Ten-Print workstation.

SYS1713 IAFIS (ITN/TPS) shall provide the capability for Authorized FBI Service Providers to mark a transaction to be held for further review during the review of the transaction in support of the PPR mode on a Ten-Print workstation.

SYS1714 IAFIS (ITN/TPS) shall provide the capability for Authorized FBI Service Providers to mark a transaction as skipped after reviewing the transaction in support of the PPR mode on a Ten-Print workstation.

3.8.11.3 Provide Latent Processing Workstation

SYS1715 IAFIS shall support all latent service functions using an IAFIS workstation.

SYS1716 IAFIS (ITN/LPS) shall provide the capability to automatically or manually extract fingerprint features on a latent workstation.

SYS1717 IAFIS (ITN/LPS) shall provide digital image processing capabilities to extract, identify, plot, and format ridge structure information on a latent workstation.

SYS1718 IAFIS (ITN/LPS) shall provide the capability to reduce noise, clarify ridges, and eliminate false fingerprint features in support of latent processing on a latent workstation.

SYS1719 IAFIS (ITN/LPS) shall allow Authorized FBI Service Providers to manually enter data in support of latent processing on a latent workstation.

SYS1720 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to view a list of all latent submissions.

The list may include the system transaction type, originator, case number, and name of the Latent Service Provider who created the requests.

SYS1721 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to assign a unique Latent Case Number (LCN) and Latent Case Extension Number (LCX) to each latent submission.

SYS1722 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider (i.e., Latent Supervisor) to assign or re-assign latent cases to one or more Service Providers on a latent workstation.

SYS1723 IAFIS (ITN/LPS) shall notify the assigned Authorized FBI Latent Service Provider when a case has been assigned to them.

SYS1724 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to apply image manipulations and enhancements using the advanced latent image processing tools in support of latent processing on a latent workstation.

SYS1725 IAFIS (ITN/LPS) shall retain the original image when applying image manipulations and enhancements in support of latent processing on a latent workstation.

SYS1726 IAFIS (ITN/LPS) shall retain all adjusted images when applying image manipulations and enhancements in support of latent processing on a latent workstation.

Each time the service provider saves an adjusted image, the previous version of that image is retained.

SYS1727 IAFIS (ITN/LPS) shall store the original image and all adjusted images until an authorized Service Provider deletes the data at the completion of case activity in support of latent processing on a latent workstation.

SYS1728 IAFIS (ITN/LPS) shall log the history of each image processing step performed on the original latent image in support of latent processing on a latent workstation.

SYS1729 IAFIS (ITN/LPS) shall provide the capability for the Authorized FBI Service Provider to view the history of all image processing steps performed on a latent image in support of latent processing on a latent workstation.

SYS1730 IAFIS (ITN/LPS) shall provide the capability for the Authorized FBI Service Provider to view all images created during image processing on a latent workstation.

SYS1731 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to select an adjusted fingerprint image for Latent Fingerprint Feature Searching in support of latent processing on a latent workstation.

SYS1732 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to print the history log in support of latent processing on a latent workstation.

NGI-432

SYS1733 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to print the image processing log in support of latent processing on a latent workstation.

SYS1734 IAFIS (ITN/LPS) shall provide the capability to print out the search fingerprint image and the candidate fingerprint image in actual size or enlarged with and without drawings, notations, and marks in support of latent processing on a latent workstation.

SYS1735 IAFIS (ITN/LPS) shall allow Authorized FBI Service Providers to modify parameters and resubmit latent searches with the modified parameters in support of latent processing on a latent workstation.

3.8.11.3.1 Latent Image Processing Tools

SYS1736 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to reverse video and switch background and foreground colors of a displayed image in support of latent processing on a latent workstation.

SYS1737 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to modify grayscale translations and remap grayscale values in support of latent processing on a latent workstation.

SYS1738 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to chart and identify and number the corresponding feature points on both latent and candidate images in support of latent processing on a latent workstation.

SYS1739 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to view the properties or attributes of an image (e.g., resolution, scale, size) in support of latent processing on a latent workstation.

SYS1740 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to register or re-orient and re-scale a fingerprint image in support of latent processing on a latent workstation.

SYS1741 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to apply image filters (including high-pass and low pass zonal, band pass, edge dilation, and erosion filters), accentuate spectral bands, remove periodic noise, adjust contrast variation, and enhance ridge structure in support of latent processing on a latent workstation.

SYS1742 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to apply kernel filters (including high-pass, low-pass, user-defined, median filters, and un-sharp masks) and perform ridge enhancement and non-linear noise reduction in support of latent processing on a latent workstation.

SYS1743 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to create a graphic representation of a histogram of pixel intensities in support of latent processing on a latent workstation.

SYS1744 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to modify a graphic representation of a histogram of pixel intensities in support of latent processing on a latent workstation.

SYS1745 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to clip an image or convert an image into a binary format in support of latent processing on a latent workstation.

SYS1746 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to crop or extract an interior sub-region of an image in support of latent processing on a latent workstation.

SYS1747 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to perform image math operations that add, subtract, and average two images, resulting in a single new image in support of latent processing on a latent workstation.

SYS1748 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to add drawings, notations, and marks to images in support of latent processing on a latent workstation.

SYS1749 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to display marked fingerprint features superimposed on the latent fingerprint image in support of latent processing on a latent workstation.

3.8.11.3.2 Provide Latent Print Scanning

SYS1750 IAFIS (ITN/LPS) shall provide the capability to scan hardcopy images into an electronic format in support of latent processing on a latent workstation.

SYS1751 IAFIS (ITN/LPS) shall provide the capability for a latent workstation to scan standard ten-print cards in support of latent processing on a latent workstation.

SYS1752 IAFIS (ITN/LPS) shall provide the capability to scan latent fingerprint submissions at 500 or 1000 pixels per inch (ppi) and 256 shades of gray on a latent workstation.

The maximum size image scanned at 500 ppi will be a set of palm prints (palm prints are normally received on eight inch by eight inch cards).

The maximum size image scanned at 1000 ppi will be 1.5 inches x 1.6 inches.

SYS1753 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to calibrate the latent image scan device in support of latent processing on a latent workstation.

SYS1754 IAFIS (ITN/LPS) shall support scanning of paper media up to 8.5 inches x 11 inches in size in support of latent processing on a latent workstation.

3.8.11.3.3 Provide Search Subject Capability

SYS1755 IAFIS (ITN/LPS) shall provide the capability for an authorized service provider to perform subject searches in support of latent processing on a latent workstation.

IAFIS will allow criminal or civil subject searches in support of latent processing.

SYS1756 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to select subject(s) from the subject search candidate list in support of latent processing on a latent workstation.

SYS1757 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to retrieve fingerprint images for subject search candidates in support of latent processing on a latent workstation.

SYS1758 IAFIS (ITN/LPS) shall mask Special Stops candidate data on the subject search candidate list as part of a subject search request prior to TPS Special Stops releasing the candidate data in support of latent processing on a latent workstation.

3.8.11.3.4 Provide Feature Extraction

SYS1759 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to manually extract fingerprint features in support of latent processing on a latent workstation.

SYS1760 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to initiate automatic fingerprint feature extraction in support of latent processing on a latent workstation.

SYS1761 IAFIS (ITN/LPS) shall display the extracted fingerprint characteristics associated with the corresponding regions of the displayed fingerprint image in support of latent processing on a latent workstation.

3.8.11.3.5 Provide Fingerprint Features Editing

SYS1762 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to perform manual fingerprint features editing (add, delete, modify) in support of latent processing on a latent workstation.

SYS1763 IAFIS (ITN/LPS) shall provide the capability to search using edited fingerprint features in support of latent processing on a latent workstation.

SYS1764 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to save fingerprint features in support of latent processing on a latent workstation.

SYS1765 IAFIS (ITN/LPS) shall provide a ridge counting capability by counting the number of ridges crossed by a straight line between two Service Provider specified minutiae points in support of latent processing on a latent workstation.

SYS1766 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to modify ridge counts in support of latent processing on a latent workstation.

SYS1767 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to edit previously marked fingerprint features in support of latent processing on a latent workstation.

SYS1768 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to edit marked fingerprint features without impacting the underlying image display in support of latent processing on a latent workstation.

SYS1769 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider editing capabilities that include addition, removal, and modification of single marks in support of latent processing on a latent workstation.

SYS1770 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to bind a region using rectangles and Service Provider defined polygons in support of latent processing on a latent workstation.

3.8.11.3.6 Provide Fingerprint Features Search Capability

SYS1771 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to initiate feature searches in support of latent processing on a latent workstation.

IAFIS will allow feature searching of criminal, civil, SLC, and ULF repositories in support of latent processing.

NGI-435

SYS1772 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider

to indicate that fingerprint images should be added to the ULF as part of a feature search on a latent workstation.

SYS1773 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to retrieve fingerprint images for feature search candidates in support of latent processing on a latent workstation.

3.8.11.3.7 Provide Creation of Ten-Print Submission for Latent Search

A latent fingerprint submission request will be a request to ITN/TPS for a latent ten-print fingerprint-based, non-retain submission. A latent ten-print fingerprint submission will result in an identification or non-identification response.

SYS1774 IAFIS (ITN/LPS) shall segment a scanned image of a ten-print fingerprint card into 14 images (ten-rolled and 4 flats) in support of latent processing on a latent workstation.

SYS1775 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to create an IAFIS Ten-print Submission using a set of fingerprint images and descriptive information in support of latent processing on a latent workstation.

SYS1776 IAFIS (ITN/LPS) shall forward an Authorized FBI Service Provider created ten-print submission to ITN/TPS for processing in support of latent processing on a latent workstation.

3.8.11.3.8 Provide Latent Fingerprint Sequence Check

ITN/LPS will support latent fingerprint image sequence checking of ten-prints submitted, for latent processing, a function called Fingerprint Sequence Check (FSC). The Fingerprint Sequence Check is used to verify that the fingerprint images on a latent ten-print submission are in the correct sequence.

SYS1777 IAFIS (ITN/LPS) shall display fingerprint images and support a comparison of rolled and plain impressions for latent fingerprint sequence checking in support of latent processing on a latent workstation.

SYS1778 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to change the sequence of the latent rolled and plain fingerprints in support of latent processing on a latent workstation.

SYS1779 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to confirm any fingerprint sequence change(s) in support of latent processing on a latent workstation.

SYS1780 IAFIS (ITN/LPS) shall maintain a history of any latent sequence changes in support of latent processing on a latent workstation.

SYS1781 IAFIS (ITN/LPS) shall display the latent sequence change history to the Authorized FBI Service Provider during sequence check processing in support of latent processing on a latent workstation.

SYS1782 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to apply a stamp to indicate the presence of a scar or amputation on any finger, if appropriate, in support of latent processing on a latent workstation.

3.8.11.3.9 Provide Manual Latent Fingerprint Classification

NGI-436

SYS1783 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider

to manually enter latent fingerprint pattern classification data in support of latent processing on a latent workstation.

SYS1784 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to enter multiple latent classifications for each finger (i.e., referencing) in support of latent processing on a latent workstation.

IAFIS will support the following latent pattern level classifications: left slant loops, right slant loops, arches, tented arches, whorls, amputations, and scarred patterns.

SYS1785 IAFIS (ITN/LPS) shall accept entry of Unable to Classify (UC) for individual fingerprints in support of latent processing on a latent workstation.

3.8.11.3.10 Provide Correlation Candidate List

The Correlation Candidate List is produced during AFIS Post Latent Processing (PLP) search to provide a list of possible candidate matches between latent searches for the same case.

SYS1786 IAFIS (ITN/LPS) shall provide an Authorized FBI Service Provider with a Correlation Candidate List (CCL).

SYS1787 IAFIS (ITN/LPS) shall provide an Authorized FBI Service Provider the capability to display the correlation information from the latent CMF searches contributing to the selection of the candidate as part of the CCL.

IAFIS will display the following information as part of the correlation information (CCL): candidate UCN, candidate descriptive data, status of each candidate, number of searches containing the same FNU/UCN, the correlation score, correlation completion data (Date/Time Stamp), the case number, the submission extension, the search and extension, the number of fingers, the finger number of highest match, the match position, the match score, present decision for the candidate, the search availability, and the image identifiers.

SYS1788 IAFIS (ITN/LPS) shall mask Special Stops candidate data on the Correlation Candidate List as part of a Latent Fingerprint Search request prior to TPS Special Stops releasing the candidate data in support of latent processing on a latent workstation.

3.8.11.3.11 Provide Latent Fingerprint Comparison

Latent Service Providers will attempt to positively identify latent fingerprints by comparing pairs of latent fingerprints in the submission with those in FBI files. Fingerprints in FBI files and submitted fingerprints will contain fingerprints for all ten fingers and possibly optional additional prints (e.g., palm prints). Latent Service Providers will compare the fingerprints, either latent or ten-print, and will respond with a decision. Latent Service Providers will use Subject Search, Ad-hoc Search, and Fingerprint Search to support Latent Fingerprint Comparison.

SYS1789 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to perform image comparison on the workstation through side-by-side display of fingerprint images for ten-print to ten-print, latent to ten-print, and latent to latent comparisons in support of latent processing on a latent workstation.

SYS1790 IAFIS (ITN/LPS) shall concurrently display fingerprint images from a latent submission with images of the corresponding fingers from a selected candidate in support of latent processing on a latent workstation.

NGI-437

SYS1791 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider

to preview all ten fingers and indicate the finger number(s) for comparison for ten-print to ten-print comparisons in support of latent processing on a latent workstation.

SYS1792 IAFIS (ITN/LPS) shall display search results as ranked by AFIS in support of latent processing on a latent workstation.

SYS1793 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to indicate a positive identification decision on a candidate in support of LFIC on a latent workstation.

SYS1794 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to indicate a non-identification decision on a candidate in support of LFIC on a latent workstation.

SYS1795 IAFIS (ITN/LPS) shall provide the capability for an Authorized FBI Service Provider to indicate an inconclusive decision on a candidate in support of LFIC on a latent workstation.

SYS1796 IAFIS (ITN/LPS) shall store candidate decision information in support of LFIC on a latent workstation

Latent Service Providers will receive latent fingerprints from users for consultation and evaluation. Latent specialists require the capability to provide their search results to other Latent Specialists for consultation and verification. A Latent Service Provider may forward the images and related information to another Latent Service Provider for verification. IAFIS will include the search results or a description of how the search results can be obtained. This action is provided in the assignment of other Latent Service Providers to review the case.

3.8.11.4 Provide Document Processing Workstation

SYS1797 IAFIS (ITN) shall support all document processing functions using an IAFIS workstation.

SYS1798 IAFIS (ITN/DPS) shall provide Human Machine Interfaces (HMIs) for an Authorized FBI Service Provider to perform document processing.

Table 3.8.11-3 shows the functional allocation for each ITN/DPS process and summarizes the requirements for manual or automated functional support.

Table 3.8.11-3 ITN/DPS Functional Allocation

ITN/DPS Process	ITN/DPS Operational Functions				
	Quality Check	Trans. Init.	Doc. IDENT	Data Entry	Auto. Edit Check
Cancel Expungement	X	X	X	X	X
CCA Modification	X	X	X	X	X
SCH Modification	X	X	X	X	X
Confirm Expungement	X	X	X	X	X
Consolidation	X	X	X	X	X
Criminal History Request	X	X	X	X	X
CRS Modification	X	X	X	X	X
Death Notice	X	X	X	X	X
Disposition	X	X	X	X	X
Expungement	X	X	X	X	X
Federal Agency Subject Search	X	X	X	X	X
Fingerprint Image Request	X	X	X	X	X

ITN/DPS Process	ITN/DPS Operational Functions				
	Quality Check	Trans. Init.	Doc. IDENT	Data Entry	Auto. Edit Check
Freedom of Information Act Record Request	X	X	X	X	X
Manual Civil File Search					
Record Sealing	X	X	X	X	X
Response Request		X	X	X	
Special Correspondence	X	X	X	X	X
Subject Search	X	X	X	X	X
Wanted Flier/IO	X	X	X	X	X
CCA Ad Hoc Search					
RANR		X	X	X	X
Restore FNU	X	X	X	X	X
Want and Flash Processing	X	X	X	X	X
Special Stop Mod	X	X	X	X	X

Table 3.8.11-3 ITN/DPS Functional Allocation (Continued)

ITN/DPS Process	ITN/DPS Operational Functions						
	Subject Search Request	FP Image Request	Update Subject File Request	Update CCA Request	Update CRS Request	FIC Request	Consol. Request
Cancel Expungement							
CCA Modification				X			
SCH Modification	X		X		X		
Confirm Expungement							
Consolidation	X				X	X	X
CRS Modification					X		
Death Notice	X		X		X		
Disposition	X		X		X		
Expungement	X		X		X		
Federal Agency Subject Search	X				X		
Fingerprint Image Request	X	X			X		
Freedom of Information Act Record Request	X	X				X	
Manual Civil File Search							
Record Sealing	X		X				
Response Request							
Special Correspondence	X	X	X		X	X	
Subject Search	X						
Wanted Flier/IO	X	X					
CCA Ad Hoc Search				X			
RANR							
Restore FNU			X			X	
Want and Flash Processing	X		X		X		
Special Stop Mod Notice	X		X				

Table 3.8.11-3 ITN/DPS Functional Allocation (Continued)

ITN/DPS Process	ITN/DPS Operational Functions							
	Record Sealing Request	Death Notice Request	Disp. Request	Expung. Request	Partial Expung. Request	Confirm Expung. Request	Cancel Expung. Request	SCH Mod. Request
Cancel Expungement							X	
CCA Modification								
SCH Modification								X
Confirm Expungement						X		
Consolidation								
Criminal History Request								
CRS Modification								
Death Notice		X						
Disposition			X					
Expungement				X	X			
Federal Agency Subject Search								
Fingerprint Image Request								
Freedom of Information Act Record								
Manual Civil File Search								
Record Sealing	X							
Response Request								
Special Correspondence								
Subject Search								
Wanted Flier/IO								
CCA Ad Hoc Search								
RANR								
Restore FNU								
Want and Flash Processing								X

Table 3.8.11-3 ITN/DPS Functional Allocation (Continued)

ITN/DPS Process	ITN/DPS Operational Functions			
	Prepare Freeform Response	Local Hardcopy Generation	Response Generation Request	CCA Ad Hoc Search
Cancel Expungement		X	X	
CCA Modification		X	X	
SCH Modification		X		
Confirm Expungement		X	X	
Consolidation		X	X	
Criminal History Request		X	X	
CRS Modification		X	X	
Death Notice		X	X	
Disposition		X	X	
Expungement		X	X	
Federal Agency Subject Search		X	X	
Fingerprint Image Request		X	X	
Freedom of Information Act Record		X	X	
Record Sealing				
Response Request		X	X	
Special Correspondence	X	X	X	
Subject Search		X	X	

ITN/DPS Process	ITN/DPS Operational Functions			
	Prepare Freeform Response	Local Hardcopy Generation	Response Generation Request	CCA Ad Hoc Search
Wanted Flier/IO		X	X	
CCA Ad Hoc Search				X
RANR		X		
Restore FNU		X	X	
Want and Flash Processing	X	X	X	

Table 3.8.11-3 ITN/DPS Functional Allocation (Continued)

ITN/DPS Process	ITN/DPS Operational Functions		
	Fingerprint Card Scan	Fingerprint Search	RANR Request
Cancel Expungement			
CCA Modification			
SCH Modification			
Confirm Expungement			
Consolidation			
Criminal History Request			
CRS Modification			
Death Notice			
Disposition			
Expungement			
Federal Agency Subject Search			
Fingerprint Image Request			
Freedom of Information Act Record Request	X	X	
Manual Civil File Search			
Record Sealing			
Response Request			
Special Correspondence	X	X	
Subject Search			
Wanted Flier/IO			
CCA Ad Hoc Search			
RANR			X
Restore FNU	X		
Want/Flash Processing Support			

3.8.11.4.1 Provide Manual Entry for Document Submissions

SYS1799 IAFIS (ITN/DPS) shall provide the capability to manually enter information into HMI(s) as part of document processing.

SYS1800 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider to initiate a system transaction as part of document processing.

SYS1801 IAFIS (ITN/DPS) shall require the Authorized FBI Service Provider to include the transaction type as part of document processing.

SYS1802 IAFIS (ITN/DPS) shall provide the capability for an Authorized FBI Service Provider

to scan fingerprint cards as part of document processing.

SYS1803 IAFIS (ITN/DPS) shall provide the capability for Authorized FBI Service Providers to segment an image of a ten-print fingerprint card into 14 images (ten rolled and four flat impressions).

SYS1804 IAFIS (ITN/DPS) shall provide the capability for Authorized FBI Service Provider to indicate whether to scan a criminal or civil fingerprint card.

SYS1805 IAFIS (ITN/DPS) shall allow an Authorized FBI Service Provider to create and initiate a ten-print submission using the entered data and scanned fingerprint and text images.

3.8.11.4.2 Provide Automated Edit Checks

SYS1806 IAFIS (ITN/DPS) shall validate manually entered system transaction data in accordance with the IAFIS ICD.

SYS1807 IAFIS (ITN/DPS) shall display the error message(s) as described in the IAFIS ICD in support of document processing.

SYS1808 IAFIS (ITN/DPS) shall allow an Authorized FBI Service Provider to correct manually entered system transaction data that is incomplete or invalid.

3.8.11.4.3 Provide Special Stop Review Processing

Special stop processing includes the review and processing of system or segment transactions whose normal processing has been suspended because the transaction involves subjects from the Subject Criminal Master File who have been deemed as requiring "special handling". When an IAFIS function detects a transaction requiring special stop processing, processing on that transaction is suspended, and a review request is send to ITN/DPS special stops. Sometimes the transaction is not suspended, but, the review request is still sent. Once notified, Service Providers at special stops will review data related to the transaction in question, perform any necessary processing, and, if necessary, signal the system to continue, thereby releasing the transaction back to normal IAFIS workflow processing. This special stop processing will be performed in accordance with the IAFIS Filtering Rules which indicate which transactions are filtered, when they are filtered, and what happens if a subject requiring "special handling" is detected.

SYS1809 IAFIS (ITN/DPS) shall provide the functions necessary to perform special stops review processing.

SYS1810 IAFIS (ITN/TPS) shall have the capability to determine when an inter-segment transaction requires special stop review processing.

Inter-segment transaction results will contain data for ITN/TPS to make this determination. The determination will be made in accordance with the *IAFIS Filtering Rules.*

SYS1811 IAFIS (ITN/TPS) shall suspend processing of a transaction requiring special stops review, as appropriate.

SYS1812 IAFIS (ITN/TPS) shall continue normal processing of a transaction after special stops releases the transaction.

According to the special stops flag, a transaction may or may not continue processing while a notification is sent to special stops for processing. NGI-442

SYS1813 IAFIS (ITN/DPS) shall receive special stops review requests and place them into a queue for review by the special stops Authorized FBI Service Providers.

SYS1814 IAFIS (ITN/DPS) shall notify special stops Authorized FBI Service Providers of new arrivals into the special stops review queue.

This is to alert special stop Service Providers of incoming work when the queue was previously empty.

SYS1815 IAFIS (ITN/DPS) shall provide the special stops Authorized FBI Service Provider the capability to display a list of all transactions and review requests received as part of special stops review processing.

SYS1816 IAFIS (ITN/DPS) shall display review transactions to special stop Authorized FBI Service Providers in the order received, by default.

SYS1817 IAFIS (ITN/DPS) shall provide the capability for a special stops Authorized FBI Service Provider to assign or re-assign transactions and requests to a specific special stops Authorized FBI Service Provider as part of special stops review processing.

The system will display the ICN, transaction type, where within IAFIS the transaction or request came from (e.g., III AFIS, ITN/ISRE, ITN/LPS, ITN/DPS, or ITN/TPS), and the last function performed (if available) to permit an authorized Service Provider to assign the transaction or request to a specific Service Provider.

SYS1818 IAFIS (ITN/DPS) shall allow special stops Authorized FBI Service Providers to select queued transactions for review and processing.

SYS1819 IAFIS (ITN/DPS) shall display all of the data for a selected system or segment transaction along with the current status to a special stops Authorized FBI Service Provider for review.

SYS1820 IAFIS (ITN/DPS) shall provide the capability for special stops Authorized FBI Service Providers to modify transaction data to complete processing of the transaction.

SYS1821 IAFIS (ITN/DPS) shall provide the capability for special stop Authorized FBI Service Providers to perform fingerprint comparisons and verification of fingerprints.

This will be used when a non-fingerprint examiner special stop Service Provider is assigned a transaction requiring fingerprint comparisons.

SYS1822 IAFIS (ITN/DPS) shall allow a special stop Authorized FBI Service Provider to scan in fingerprint cards and enter data for processing.

This allows special stop Service Providers to process ITN/TPS and ITN/DPS system transactions from beginning to end; to receive ITN/TPS and ITN/DPS system transactions and process them to completion; and to receive ITN/TPS and ITN/DPS system transactions, perform the necessary processing functions and then, pass them back to the normal work flow for completion.

SYS1823 IAFIS (ITN/DPS) shall provide the capability for a special stops Authorized FBI Service Provider to request records from the Fingerprint Image Master File (FIMF) by FNU for comparison with a stopped ten-print submission.

SYS1824 IAFIS (ITN/DPS) shall provide the capability for special stops Authorized FBI Service Providers to add, modify, or delete special stop flags on subject records in the Subject Criminal History File.

SYS1825 IAFIS (ITN/DPS) shall provide the capability for special stops Authorized FBI Service Providers to direct response generation to a local printer within special stops.

In most cases response generation will be left to the default rules in III.

SYS1826 IAFIS (ITN/DPS) shall provide the capability for special stops Authorized FBI Service Providers to release the transaction into normal work flow for completion.

3.8.11.4.4 Provide Special Stops Processing

The special stops Service Provider will have the ability to retrieve FIMF records, select individual fingerprint images from multiple FIMF records or all images from single FIMF record to create a new, unique, composite, fingerprint "card". The images used to create the composite fingerprint "card" can be placed in any sequence. The composite fingerprint "card" will be used to create a new subject or update an existing subject record.

SYS1827 IAFIS (ITN/DPS) shall provide the capability for special stops Authorized FBI Service Providers to request records from the FIMF in order to create a new, unique, composite, criminal fingerprint records.

SYS1828 IAFIS (ITN/DPS) shall allow the special stops Authorized FBI Service Provider to select individual finger images from multiple FIMF records or all images from a single FIMF record to create a new composite criminal fingerprint record.

SYS1829 IAFIS (ITN/DPS) shall allow the special stops Authorized FBI Service Provider to copy the finger images in any sequence to create a new composite criminal fingerprint record.

SYS1830 IAFIS (ITN/DPS) shall allow the special stops Authorized FBI Service Provider to submit updates to the FIMF using the new composite fingerprint record.

SYS1831 IAFIS (ITN/DPS) shall allow the special stops Authorized FBI Service Provider to submit a transaction to AFIS for updates to the Criminal Ten-print Fingerprint Features Master File (CMF) using the new composite fingerprint record.

SYS1832 IAFIS (ITN/DPS) shall provide the capability for special stop Authorized FBI Service Providers to enter subjects' entire textual record including subjects' identification data, arrest criminal history data, court data, additional court data, and custody/supervisory data.

SYS1833 IAFIS (ITN/DPS) shall provide the capability for special stop Authorized FBI Service Providers to submit a file maintenance request to III for entry into the III Subject Criminal History File.

SYS1834 IAFIS (ITN/DPS) shall provide the capability for special stop Authorized FBI Service Providers to designate a new FBI Number to be assigned to the new composite fingerprint record for the created subject identification record.

3.8.11.4.5 Provide Want/Flash Processing

SYS1835 IAFIS (ITN/DPS) shall place want hit notifications into a queue for review by the want/flash Authorized FBI Service Provider.

SYS1836 IAFIS (ITN/DPS) shall notify authorized want/flash Authorized FBI Service Providers of new arrivals in the want/flash queue.

SYS1837 IAFIS (ITN/DPS) shall provide the capability for a want/flash Authorized FBI Service Provider to view a list of all transactions requiring review.

SYS1838 IAFIS (ITN/DPS) shall provide the capability for a want/flash Authorized FBI Service Provider to assign or re-assign want/flash transactions requiring review.

SYS1839 IAFIS (ITN/DPS) shall allow want/flash Authorized FBI Service Providers to select queued want/flash transactions.

SYS1840 IAFIS (ITN/DPS) shall display all of the text data and the current status for the selected transaction to a want/flash Authorized FBI Service Provider for review.

SYS1841 IAFIS (ITN/DPS) shall present review transactions to want/flash Authorized FBI Service Providers in response time order, such that, the earliest response time is processed first.

SYS1842 IAFIS (ITN/DPS) shall provide the capability for a want/flash Authorized FBI Service Provider to modify a selected want/flash transaction for continued processing.

SYS1843 ITN/DPS shall provide the capability for a want/flash Authorized FBI Service Provider to send a response release to III.

4 SYSTEM OPERATIONAL REQUIREMENTS

This section describes the non-functional requirements, or general operational characteristics of the IAFIS as a whole.

4.1 Security

This section describes the IAFIS data confidentiality and data integrity requirements. IAFIS security requirements are based on the security policy, threats, and system configuration.

The provisions of the Privacy Act of 1974 and the Computer Security Act of 1987, levy certain requirements on departments and agencies of the executive branch of the Federal Government. The Privacy Act specifies that information should be protected against unauthorized access, alteration, or distribution. The Computer Security Act mandates that a System Security Plan must be prepared for all information systems in the Federal Government that store or process sensitive information. The IAFIS security requirements are based upon the CJISCAPP, the FBI MIOG Part II, Section 35, and *DOD 5200.28-STD*.

SYS1844 IAFIS shall comply with the security policies, recommendations, and requirements of the most recent version of the Criminal Justice Information Services Controlled Access Protection Profile (CJISCAPP).

SYS1845 IAFIS shall comply with the security policies, recommendations, and requirements of the most recent version of the Manual of Investigative Operations and Guidelines (MIOG).

SYS1846 IAFIS shall comply with 5 U.S. Code 552a, Privacy Act of 1974 (Public Law 93-579).

SYS1847 IAFIS shall comply with 40 U.S. Code 759, Computer Security Act of 1987, (Public Law 100-235), January 8, 1988.

SYS1848 IAFIS shall comply with the security policies, recommendations, and requirements of the most recent version of the FBI Security Division Security Requirements Traceability Matrix (SRTM).

SYS1849 IAFIS shall operate as an Information Technology (IT) security Certification and Accreditation (C&A) system.

SYS1850 IAFIS shall process only non-classified (UNCLASSIFIED) information that has been designated as Sensitive but Unclassified (SBU) information.

SYS1851 IAFIS shall operate in a highly secure mode of operation.

SYS1852 IAFIS shall provide the capability to detect, recognize, and address system threats.

SYS1853 IAFIS shall provide the capability to prevent unauthorized access to the system.

The IAFIS user community will be considered a "non-hostile" user community that requires protection against inadvertent threats or casual attempts to breach system security. Access to IAFIS is controlled by rules that restrict individual users according to their system defined roles

or organizational membership and need-to-know requirements. The System Security Administrator has the responsibility for ensuring that all users are assigned their proper role(s).

4.1.1 IAFIS Direct User Accessibility

From the security perspective, IAFIS will have two types of users: direct users, and indirect users. Direct users are those who login to an IAFIS segment with an interactive session, including operators, service providers, and specialists. Indirect users submit messages through NCIC, Nlets, or the CJIS WAN but do not have interactive sessions. Throughout this section, a reference to "users" refers to both direct and indirect users. Each user must be accountable for the system, inter-segment, and intra-segment transactions they initiate or request in IAFIS. Unique user identification and authentication not only prevents unauthorized users from gaining access to the system, but also ensures user accountability for all of the system, inter-segment, and intra-segment transactions that are associated with an identifier.

SYS1854 IAFIS shall provide direct user identification and authentication for controlling access to IAFIS.

4.1.1.1 IAFIS Roles and Privileges for Direct Users

IAFIS will prevent a direct user from executing any process or function or assuming any role not specified in the user's profile or implicit in any roles or organizational memberships associated with the identifier.

SYS1855 IAFIS shall provide direct users with access to IAFIS functions, processes, and objects based upon assigned user profiles.

SYS2256 IAFIS (iDSM) shall provide the capability to uniquely identify each direct user thus ensuring individual accountability.

SYS1856 IAFIS shall support Authorized FBI Service Provider workgroup assignments.

The IAFIS staffing workload will be distributed among organized workgroups, where feasible. The FBI will provide a work atmosphere that encourages the evolution of the self-directed workgroup.

SYS1857 IAFIS shall support an organizational structure consisting of Operations Managers, Area Supervisors, Team Leaders, and Authorized FBI Service Providers.

SYS1858 IAFIS shall automatically verify all data service requests to ensure that the requestor has access authority for the function and the record.

SYS1859 IAFIS shall reject unauthorized data service requests and supply status indications.

SYS1860 IAFIS shall support workgroup processing.

SYS1861 IAFIS shall be capable of automatically assigning tasks to direct users for processing in a manner consistent with the person's assigned role.

SYS1862 IAFIS shall control direct user access to the IAFIS processes by assigning a role to each direct user.

SYS1863 IAFIS shall control direct user access to the IAFIS processes by assigning permissions to each user role.

NGI-447

SYS1864 IAFIS (ITN) shall assign a skill level to AFIS for fingerprint comparison.

This skill level will be used for III/Verify and Feature Search functions. ITN will create an EID with the assigned skill level to be used during the recording of the decision in Transaction History.

SYS1865 IAFIS (ITN) shall support a four-tier skill level structure (i.e., Level 1—FBI Service Provider, Level 2—Experienced FBI Service Provider/team leader, Level 3—Area Supervisor, Level 4—Operations Manager).

The Operations Manager will control the operation of IAFIS by making decisions concerning policy and organizational procedures. These decisions affect the following production capabilities: types of workflows to be established and types of work groups that need to be formed.

SYS1866 IAFIS (ITN) shall provide management reports on an as-needed basis to the Operations Manager to assist in making decisions.

Area Supervisors will oversee multiple work groups and the Team Leaders responsible for these work groups. Area Supervisors will coordinate activities among themselves, standardize instructions to Team Leaders for off-nominal conditions, and report directly to the Operations Manager. Area Supervisors are responsible for the quality of work and productivity of each work group that they supervise. They will have the following responsibilities:

- Determine the number and size of work groups needed,
- Define the appropriate workflows and profiles, and
- Coordinate system level responses to off-nominal conditions.

SYS1867 IAFIS (ITN) shall provide management reports on an as-needed basis to the Area Supervisors to assist in managing the work groups assigned to them along with the accompanying workloads.

Team Leaders will be responsible for managing one work group and the FBI Service Providers within the work group. The Team Leader's main objective is to control the productivity and quality of the work group assigned to them. Team Leaders will have the following responsibilities:

- Monitor workgroup and FBI Service Provider productivity to identify trends and mitigate problems,
- Assure that work group and FBI Service Provider profiles meet processing needs, and
- Review FBI Service Provider actions and performance.

SYS1868 IAFIS (ITN) shall provide tools on an as-needed basis to the Team Leaders to assist in managing their work groups assigned to them (e.g., access historical reports, review forwarded and rejected submissions, review transactions in-process).

FBI Service Providers will perform the actual day-to-day processing of submissions. Each FBI Service Provider has a profile that specifies the functions s/he is authorized to perform. FBI Service Providers will receive direction from their Team Leader as to the function to perform.

Service Providers will access IAFIS services and data using IAFIS ITN SPWs. Typically, authorized Service Providers will be CJIS personnel who access the IAFIS databases via HMIs.

Service Provider profiles will be established to restrict data access and modifications based upon operational need. Service Provides may be given more than one profile based on supervisor approval. The Service Provider profiles are depicted in Table 4.1.1-1

Table 4.1.1-1 Service Provider Profiles

Service Provider Operations		
Roles	**Functions**	**Applications**
• Area Supervisor • Latent Specialist • Latent Supervisor • Operations Supervisor • Service Provider • Systems Administrator • Teamlead	TPS	-Fingerprint Image Compare -Fingerprint Sequence Check -Logic Error Resolution -Quality Check
	DPS	-Consolidation PPR Mode -Consolidation Queue -Criminal History Modification -Disposition -Expungement -Forward FNU -Master Record Conversion -Record Seal -Restore FNU
	LPS	-AFIS Latent Search -AFIS Search Candidate List -AFIS Ten Print Search -Assign Submission Log -Edit Image Text -Edit Submission -Enter Batch Data -Evaluate Image -Forward to TPS -Image Compare -Image Log -Image Retrieval List -Latent Feature Editor -Latent Files -Modify SLC Access and Authorization -Retrieve Image -Scan Known -Scan Latents -Search Status -Search Status and Modification Query -SLC File Maintenance -Subject Search -Subject Search Candidate List -Submission Log -Ten Print Cert File Processing -Enable/Delete Submission

Service Provider Operations		
Roles	**Functions**	**Applications**
	LOGS	-Answer Hits to Wants -Document Specialist -Service Desk -Special Correspondence -Special Stops
	DB	-ITN Transaction Statistics Reporting -Management Information Reporting -NSM Maintenance -User Fee Billing -IDWH User Fee Billing
	General	-Adhoc Subject Search -Calibrate Scanner -Contributor Data Update -CRS Update -Image Request Log -ORI Query -Print Fingerprint Images -Print Submission Images -Print Ten-print Certification Images -Reports -Subject Search
	WFM	-Workflow Queue Monitor – Restricted -Workflow Queue Monitor - Unrestricted

4.1.1.1.1 Support Work Group Units

SYS1869 IAFIS (ITN) shall support work group units consisting of Authorized FBI Service Providers and one or more team leaders.

Each work group member will perform a manual function with the aid of automated tools.

SYS1870 IAFIS (ITN) shall support Functional Work Groups consisting of Authorized FBI Service Providers and one or more team leaders that will perform one or more functions.

The particular composition of a work group will be flexible and allow work group reorganization (configuration changes). Each work group member will perform one or more functions in a work group. The team leader will monitor productivity and quality of the work group.

SYS1871 IAFIS (ITN) shall provide the capability for Authorized FBI Service Providers to access historical management reports.

Historical Management Reports are comprised of aggregated data on the performance of workgroups, FBI Service Provider productivity, identify trends, and mitigate problems.

Historical Management Reports will be presented at a system-wide or workgroup level, on the basis of the authorization of the requesting authorized FBI Service Provider. Table 4.1.1-2 describes the type of content that may be contained in a historical report.

NGI-450

Table 4.1.1-2 Historical Management Reports

Type of Report	Content
Historical	• Functions performed • Number of transactions performed by function (e.g., FIC, QC) • Function start times • Function completion times • Average response time by transaction type • Workgroup that performed each function • Workgroup member that performed each function • Workgroup and FBI Service Provider productivity • Number of transactions processed • Number of transactions forwarded • Number of transactions rejected • Number of errors • Number of redirects • Response time performance • Average time to process a transaction • Performance for workgroup members

SYS1872 IAFIS (ITN) shall provide a work group profile that will contain a list of functions that can be performed by the work group.

SYS1873 IAFIS (ITN) shall provide the ability to group work groups into logical "areas."

Work group "areas" will be managed by authorized FBI Service Providers (Area Supervisors) having the proper authorization privileges defined in their profile.

SYS1874 IAFIS (ITN) shall operate with a minimum of 1 work group.

SYS1875 IAFIS (ITN) shall operate with a maximum of 400 work groups.

SYS1876 IAFIS (ITN) shall provide a work group that will support a minimum of 1 Authorized FBI Service Provider.

SYS1877 IAFIS (ITN) shall provide a work group that will support a maximum of 250 Authorized FBI Service Providers.

SYS1878 IAFIS (ITN) shall maintain a work group status file which contains the work group identifier, the work group shift assignment, the Authorized FBI Service Provider availability (e.g., on-line/not on-line), the current work group processing capacity (e.g., Potential/Actual), and other authorized functions.

SYS1879 IAFIS (ITN) shall provide the capability for a System Administrator to update work group files.

SYS1880 IAFIS (ITN) shall provide the capability for workgroup reassignment of Authorized FBI Service Providers.

SYS1881 IAFIS (ITN) shall have an Authorized FBI Service Provider profile for each work group member that will list the functions for which the Authorized FBI Service Provider is authorized to perform.

Within a work group, work group members will be free to perform any function listed in their worker profiles at the direction of their team leader.

SYS1882 IAFIS (ITN) shall limit an Authorized FBI Service Provider to one assigned work group at a time.

NGI-451

4.1.1.1.2 Support Operational Personnel

SYS1883 IAFIS (ITN) shall provide the capability for a System Administrator to maintain and modify an Authorized FBI Service Provider profiles.

SYS1884 IAFIS (ITN) shall provide an Authorized FBI Service Provider profile data which includes name and EID, functional qualifications, work assignment, transaction review percentage, and skill levels for an Authorized FBI Service Providers for each qualified function (an Authorized FBI Service Provider can have a different skill level for each function).

SYS1885 IAFIS (ITN) shall provide the capability for a System Administrator to maintain and modify work group profiles.

SYS1886 IAFIS (ITN) shall provide work group profile data to include the number of members in work group, the number of members doing each function, a list of services provided by the work group, and an indication that rejected submissions be saved for subsequent review by the Team Leader.

4.1.1.2 IAFIS Login and Authentication for Direct Users

SYS1887 IAFIS (ITN) shall provide a unique login capability for each Authorized FBI Service Provider.

An Authorized FBI Service Providers login will include both a unique identifier and password.

SYS1888 IAFIS (ITN) shall authenticate the Authorized FBI Service Provider using an assigned unique identifier and password during each login attempt.

SYS2257 IAFIS shall encrypt all personal authenticators at the point of login.

SYS2258 IAFIS shall transmit and compare personal authenticators in an encrypted format.

SYS2259 IAFIS shall encrypt personal authenticator file using a "one-way" encryption (i.e., the key shall be embedded in the personal authenticator).

SYS1889 IAFIS shall provide the System Security Administrator with the ability to enable or disable logon access, change passwords, and specify audit parameters and access privileges for any authorized user.

The System Security Administrator will have the capability to delegate some or all System Security Administrator role privileges to specific users who may, if so stipulated by the System Security Administrator, further delegate such privileges. Delegation of privileges will always be hierarchical, with the System Security Administrator at the top of the hierarchy.

SYS1890 IAFIS (ITN) shall display the date, time, workstation identifier, and facility of the last login attempt for the authenticated FBI Service Provider.

SYS2260 IAFIS (iDSM) shall display the following security banner prior to the entry of the identifier and personal authenticator:

"WARNING! This computer system is property of the United States Government (the property of the Federal Bureau of Investigation (FBI)). The FBI may monitor any activity on the system and search, retrieve and disclose any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no

expectation of privacy as to any communication on or information stored within the system, including information stored on the network or stored locally on the hard drive or other media in use with this unit (e.g., floppy drives, CD-ROMs, etc.)."

SYS1891 IAFIS shall display encrypted passwords to direct users who are logging in or changing passwords.

SYS1892 IAFIS (ITN) shall require Authorized FBI Service Providers to change their password at the expiration of a time period specified by the System Security Administrator.

SYS1893 IAFIS shall notify a user in advance that a change of password is required.

IAFIS will automatically notify direct users in advance that a change of their password is required. The system will generate an audit record when an authenticator has exceeded its maximum lifetime and prevent such individuals from performing a login until the System Security Administrator changes the personal authenticator. In addition, the System Security Administrator will be able to change an individual's personal authenticator without having to know the individual's current password.

SYS1894 IAFIS shall prohibit access to users attempting to login using an invalid or expired login ID or password.

SYS1895 IAFIS (ITN) shall require an Authorized FBI Service Provider password to be compliant with the CJIS CAPP.

SYS1896 IAFIS shall require that user passwords meet the minimum password length requirements.

SYS1897 IAFIS shall require that user passwords meet the password complexity requirements.

SYS1898 IAFIS shall verify that user passwords are not a vendor or default password.

SYS2261 IAFIS shall change all vendor and/or default passwords.

SYS1899 IAFIS (ITN) shall prohibit the reuse of the last five passwords used by an individual Authorized FBI Service Provider.

SYS1900 IAFIS (ITN) shall store the Authorized FBI Service Provider passwords in encrypted form in a protected personal authenticator file.

IAFIS will ensure that encryption will be by "one-way" encryption, i.e., the key will be embedded in the personal authenticator.

SYS1901 IAFIS shall display a notification to a direct user when a login ID or password is invalid.

SYS2262 IAFIS shall provide a help function to assist direct users in establishing a new personal authenticator.

4.1.1.3 Provide Role Based Access Control for Direct Users

SYS1902 IAFIS (ITN) shall enforce access control rules to ensure that system processes, functions, and data objects are accessed only by Authorized FBI Service Providers or Authorized System Administrators, as explicitly defined by assigned role or organizational membership.

All attempts to modify, violate, or circumvent role based access control rules will generate a security audit record.

4.1.1.4 Prevent Multiple Simultaneous IAFIS Logins by Direct Users

SYS1903 IAFIS (ITN) shall prohibit Authorized FBI Service Providers from logging into IAFIS more than once concurrently.

SYS1904 IAFIS (ITN) shall display a notification to an Authorized FBI Service Providers attempting to perform a multiple, concurrent login that the action is prohibited and that system access is denied.

As defined by the System Security Administrator, the system will prevent a direct user from logging in more than once without first properly terminating a session as defined by the System Security Administrator. All unsuccessful attempts to login will generate a security audit record.

4.1.2 Indirect User Accessibility

IAFIS indirect users submit messages through NCIC, Nlets, or the CJIS WAN but do not have interactive sessions. Access to the IAFIS is controlled by rules that restrict individual users according to their organizational membership and need-to-know requirements.

SYS1905 IAFIS shall provide indirect user identification for controlling access to IAFIS.

SYS1906 IAFIS shall authenticate indirect users by comparing the ORI in the system transaction with specified data in the ORI Validation file.

SYS1907 IAFIS shall control indirect user access to the IAFIS processes by assigning permissions to each ORI.

4.1.2.1 Provide Secure IAFIS Access to Indirect Users

SYS1908 IAFIS shall ensure that all arriving messages from external IAFIS systems request only those functions and data authorized to the originator of the message.

SYS1909 IAFIS shall perform indirect user identification and authorization functions before allowing access.

SYS1910 IAFIS shall perform indirect user identification as specified in the CJIS CAPP.

SYS1911 IAFIS shall perform indirect user authorization as specified in the CJIS CAPP.

SYS1912 IAFIS shall support multiple, simultaneous, logical connections with external systems.

4.1.2.2 Communications Control

This section identifies requirements for IAFIS message access, traffic control, and security measures that enhance the Indirect User identification and authentication protection services provided by the CJIS WAN, NCIC and Nlets networks.

SYS1913 IAFIS shall require all remote messages from indirect users, not authenticated directly by IAFIS, to be inspected by a message access control function.

This function will ensure that:

- Every received message has a valid ORI, and is a message type and purpose code for which the ORI has authorization,

NGI-454

- Every received message is uniquely identified and logged as to date and time of receipt; and
- No part of any message can be executable or can attempt to circumvent normal processing or gain access to privileged system functions.

SYS1914 IAFIS shall require that every received message has a valid ORI, message type and purpose code for which the contributor has authorization.

SYS1915 IAFIS shall reject system transactions that do not include an ORI and an authorized, valid transaction type.

SYS1916 IAFIS shall record a security event and create an audit record of system transactions that do not include an ORI and an authorized, valid transaction type.

SYS1917 IAFIS shall prohibit any message from circumventing normal processing.

SYS1918 IAFIS shall prohibit any message from gaining access to privileged system functions without authorization.

SYS1919 IAFIS (EFCON) shall require a generated response to be matched against the message that requested a response before returning the response.

SYS2263 IAFIS shall generate an appropriate notification if a security violation occurs.

4.1.3 Security Administration

SYS1920 IAFIS shall support security administration by the System Security Administrators, each of whom will define and control direct user authentication, profiles, roles, and data access rights as well as workstation functions.

IAFIS will have numerous FBI service providers and operators. In addition, specialists from federal agencies may have direct access to IAFIS. More than one direct user may use the same IAFIS workstation in the course of a 24-hour day and the workstation may support a variety of functions. The System Security Administrator (SSA) will be able to execute these responsibilities from a central location.

SYS1921 IAFIS shall provide the capability for a SSA to disable a terminal, workstation, or access port.

SYS1922 IAFIS shall provide a direct user login/maintenance function for direct SSA access.

IAFIS Security Administration functionality will allow System Security Administrators to provide support to FBI Service Providers by allowing the Administrators to add, modify, and delete User IDs and Passwords. In addition, Security Administrators will have the ability to limit system access to those individuals who have been both identified and authenticated.

SYS1923 IAFIS shall provide the capability for the SSA to deny or allow access to system resources, and to monitor local transactions.

SYS1924 IAFIS shall provide the capability for an SSA to administer and control the system operations.

The IAFIS SSA will be at the top of the SSA hierarchy. Any SSA higher in the hierarchy will be able to control all access privileges for all personnel lower in their hierarchy.

NGI-455

SYS1925 IAFIS shall provide the capability for the SSA to define and control user

authentication, access profiles, security administration and other roles, and data access rights.

SYS1926 IAFIS shall provide the capability for the SSA to define and assign different levels of user access.

SYS1927 IAFIS shall provide the capability for the SSA to assign privileges.

SYS1928 IAFIS shall provide the capability for the SSA to assign user identifiers and passwords.

SYS1929 IAFIS shall provide the capability for the SSA to set restrictions on creating, modifying, and deleting files and directories.

SYS1930 IAFIS shall provide the capability for the SSA to establish roles and organizational groups.

SYS1931 IAFIS shall provide the capability for the SSA to specify access privileges.

SYS1932 IAFIS shall provide the capability for the SSA to enable and disable logon access.

SYS1933 IAFIS (ITN) shall automatically log off an IAFIS direct user that has been inactive for a specified number of minutes.

SYS1934 IAFIS shall allow an SSA to set the number of minutes for an inactive session logout period.

SYS1935 IAFIS shall allow an SSA to add, modify, or delete direct user access privileges.

SYS1936 IAFIS shall allow an SSA to add, modify, or delete indirect user access privileges.

SYS1937 IAFIS shall allow an SSA to add, modify, or delete a direct user account.

SYS1938 IAFIS shall allow an SSA to add, modify, or delete an indirect user account.

SYS1939 IAFIS shall allow an SSA to add, modify, or delete a direct user authenticator (password).

SYS2264 IAFIS shall allow the SSA to change a direct user's personal authenticator without having to know the current personal authenticator.

SYS1940 IAFIS shall allow an SSA to add, modify, or delete an indirect user authenticator (CRI/ORI).

SYS1941 IAFIS shall allow an SSA to add, modify, or delete a direct user role assignment.

SYS1942 IAFIS shall allow an SSA to add, modify, or delete an indirect user role assignment.

SYS1943 IAFIS shall allow an SSA to install or remove software.

SYS1944 IAFIS shall allow an SSA to monitor system performance and system usage.

SYS1945 IAFIS shall allow an SSA to alter the scope and extent of audit activities.

SYS1946 IAFIS shall allow an SSA to retrieve and review audit data.

SYS2265 IAFIS shall provide the capability for the SSA to selectively audit the actions of any direct user based on individual identity.

SYS1947 IAFIS shall allow an SSA to designate the security administrator role and associated privileges other than root privileges, to a specific individual.

NGI-456

SYS1948 IAFIS shall allow an SSA to designate if an individual who has received security

privileges may further designate those privileges to another individual.

4.1.4 System Auditing

SYS1949 IAFIS shall log all system level activity (e.g., logins, functions) that occurs within IAFIS in a system audit trail.

SYS1950 IAFIS shall provide the capability of associating a user with all auditable actions performed by that individual.

SYS1951 IAFIS shall ensure that every received message is uniquely identified and logged with date and time of receipt.

SYS1952 IAFIS shall protect the IAFIS audit data from unauthorized access, modification, or destruction.

The audit data will be protected by the system so that read access to it is limited to those who are authorized to access audit data. The SSA will be able to selectively audit the actions of any direct or indirect user based on the identifier.

The SSA will review audit data at a workstation, to determine what transactions are to be audited, to query the audit trail, to designate the time period in which audit data is to be preserved, to cause an audit trail for one or more workstations to be kept locally or at a central place, and to consolidate the various audit trails.

4.1.5 Security Auditing

SYS1953 IAFIS shall log all security related activity that occurs within IAFIS in a security audit trail.

For each audited event, the audit record will include auditable information (e.g., type of event, the date and time of the event, requester's identifier associated with the event). For identification/authentication events, the origin of the request (service provider and operator identifier and terminal identifier) will be included in the audit record.

SYS1954 IAFIS shall provide segment level audit log data in a consolidated format.

The SSA will be able to access each segment's consolidated audit data from a single segment terminal, workstation, or console without specifying where the audit trail is physically located.

SYS1955 IAFIS shall provide automatic evaluation, selection, recording, and review and analysis of information concerning security events.

SYS1956 IAFIS shall provide alarms for an SSA upon detection of a potential security violation.

SYS1957 IAFIS shall provide the capability for an SSA to determine a specific user or group that caused an auditable security event.

SYS1958 IAFIS shall provide the capability for an SSA to select audit data for review.

SYS1959 IAFIS shall prevent the unauthorized access, modification, or destruction of audit data.

4.1.6 System and Data Integrity

4.1.6.1 System Integrity

SYS1960 IAFIS shall ensure that information is protected from improper disclosure and that the services and resources composing IAFIS are impenetrable to unauthorized individuals.

A major IAFIS security goal is to ensure that the information remains as received unless changed through authorized processes and procedures.

SYS1961 IAFIS shall provide hardware features for use to periodically validate the correct operation of the on-site hardware and firmware elements.

SYS1962 IAFIS shall provide software features for use to periodically validate the correct operation of the on-site hardware and firmware elements.

SYS1963 IAFIS shall ensure that all application software executing in the operational environment is free of any debug or system interrupt functions used to test or develop the software.

SYS2266 IAFIS shall ensure that the mechanisms for enforcing the transaction rules cannot be compromised.

SYS1964 IAFIS shall maintain a separate security domain to protect security relevant software from external interference or tampering.

SYS1965 IAFIS shall limit access to the security domain by utilizing access controls.

The security domain will be subject to an auditing process.

SYS1966 IAFIS shall provide the capability to validate the correct operation of the security relevant software.

SYS1967 IAFIS shall prohibit the circumvention of the security features and access control mechanisms of the system.

4.1.6.2 Data Integrity

SYS1968 IAFIS shall ensure that specified data items can only be accessed through transaction routines that correctly enforce the transaction rules.

SYS1969 IAFIS shall ensure that each transaction is consistent with the role(s) assigned to an individual requester.

IAFIS will ensure that, the mechanisms enforcing the transaction rules cannot be compromised.

4.1.7 Application Software Assurance

SYS1970 IAFIS shall require that all application software satisfy the security features and access control mechanisms of IAFIS.

SYS1971 IAFIS shall require that all application software satisfy the authentication guidelines of the system.

SYS1972 IAFIS shall detect malicious code entering the IAFIS environment (e.g., automated baseline tools, or virus detection tools). NGI-458

SYS1973 IAFIS shall prevent malicious code from entering the IAFIS environment (e.g., automated baseline tools, or virus detection tools).

SYS2267 IAFIS shall maintain a security-relevant software domain for its own execution that is protected from external interference or tampering.

SYS2268 IAFIS shall provide an application software executing in the Operational Environment free of any debug or system interrupt functions used to develop and test the software.

SYS2269 IAFIS shall provide the capability to remove or alter vendor supplied user identification and authentication entries immediately after a component is installed.

SYS2270 IAFIS shall provide features that can be used to periodically validate the correct operation of the hardware and firmware elements of the security-relevant software.

4.1.8 Workstation Security

This section defines the security requirements applicable to IAFIS workstations. The purpose of these requirements is to prevent the unauthorized introduction, access, or deletion of software or data from IAFIS. Additional workstation security measures are intended to protect hardware from tampering by unauthorized personnel, and to ensure that direct access to the IAFIS is limited to authorized personnel only.

SYS1974 IAFIS shall require a time-out at a terminal or workstation after a specified period of inactivity.

SYS2271 IAFIS shall provide the capability for the SSA to specify the inactivity time-out period.

The inactivity time-out period of the workstations supporting shared data activities is prohibited from exceeding twenty minutes.

SYS1975 IAFIS shall prohibit workstations from having any connection from outside the IAFIS environment without prior authorization from the System Security Administrator.

IAFIS workstations will have no dial-up capabilities without the prior authorization of the System Security Administrator.

4.1.9 IAFIS Clock Synchronization

SYS1976 IAFIS (ITN) shall implement a master clock that will be synchronized with an external standard reference time, such as the Universal Coordinated Time (UTC), with an accuracy better than 0.05 seconds.

SYS1977 IAFIS (ITN) shall distribute the master clock time to all IAFIS segments and ITN elements and sub-elements using the Network Time Protocol (NTP) Version 3 of the Internet Protocol suite, RFC 1305.

4.1.10 Safeguard Against Object Reuse

NGI-459

SYS1978 IAFIS shall revoke all authorizations to the information contained within an electronic

media prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused storage objects.

No information, including encrypted representations of information provided by a prior subject's actions, would be available to any subject that obtains access to an object that has been released back to the system.

4.1.11 Provide Self-Protective System Architecture

SYS1979 IAFIS shall provide for security-relevant software to maintain a domain for its own execution that protects itself from external interference or tampering (e.g., by modification of its code or data structures).

The resources to be protected by the security-relevant software will be isolated so that they are subject to the access control and auditing requirements.

4.2 Reliability

Reliability is the probability that a system will be able to process work correctly and completely without being aborted. Reliability is defined in terms of the system processing and fingerprint matching accuracy.

4.2.1 System Reliability

System reliability for IAFIS is the probability that the system will completely process all transactions under any condition.

SYS1980 IAFIS shall process all fingerprint transactions to completion.

SYS1981 IAFIS shall process all latent transactions to completion.

SYS1982 IAFIS shall process all document transactions to completion.

4.2.1.1 Hardware Reliability

SYS1983 IAFIS shall provide hardware Mean-Time-Between-Maintenance-Actions (MTBMA) of 1,000 hours.

4.2.1.2 Software Reliability

Software reliability requirements are defined in terms of the number of unresolved errors as a function of their priorities. A software error is the inability to meet a requirement because of programming failure. Software errors are prioritized as follows:

a. Priority 1: An error that prevents a function from performing as required (e.g., causes a program stop, produces an unusable product, or produces no product).

b. Priority 2: An error that degrades the performance of a function as defined by applicable specifications and for which a reasonable alternative work-around solution is known to exist. However, a reload or restart of the program is not considered an acceptable work-around.

c. Priority 3: All other errors, including intermittent errors and those causing operator

inconvenience or annoyance but do not affect operational functions. An intermittent error is an error that cannot be reproduced consistently even when the same procedures and database(s) are used.

SYS1984 IAFIS shall measure software reliability in terms of the number of software errors that remain unresolved upon completion of the software quality testing.

SYS1985 IAFIS shall prioritize the severity of software errors as three priority levels, from one to three.

SYS1986 IAFIS shall allow zero Priority 1 software errors.

SYS1987 IAFIS shall allow one Priority 2 software error per 40k of executable lines of code (LOC).

SYS1988 IAFIS shall allow one Priority 3 software error per 20k of executable lines of code (LOC).

4.2.2 Accuracy

Accuracy is the probability that the correct identity will be selected as a candidate by IAFIS provided that the identity exists in the repository being searched; and, that no candidate will be selected if the identity is not in the repository being searched.

SYS1989 IAFIS (AFIS) shall have a minimum ten-print search accuracy of 95 percent (applied to the full-sized fingerprint file) during the fingerprint search stage of ten-print processing.

SYS1990 IAFIS (AFIS) shall produce ten-print fingerprint search reliability results, on average, a maximum of one false candidate for each ten-print search.

SYS2272 IAFIS (iDSM) shall have a minimum True Acceptance Rate (TAR) in support of data sharing that is consistent with the minimum fingerprint search reliability of 95 percent.

SYS2273 IAFIS (iDSM) shall have a maximum False Acceptance Rate (FAR) in support of data sharing that is consistent with the IAFIS selectivity no greater than 1 on average.

SYS1991 IAFIS (AFIS) shall exclude fingerprint submissions that cannot be classified because of missing characteristics when determining search reliability.

SYS1992 IAFIS (AFIS) shall include misreported data as part of the search reliability calculation.

SYS1993 IAFIS (AFIS) shall include data entry errors as part of the search reliability calculation.

SYS1994 IAFIS (AFIS) shall include fingerprint classification errors in file records as part of the search reliability calculation.

SYS1995 IAFIS (AFIS) shall include fingerprint classification errors in search records as part of the search reliability calculation.

SYS1996 IAFIS (AFIS) shall include less than high quality images as part of the search reliability calculation.

The following accuracy requirements are specific to the Automated Sequence Check function:

SYS1997 IAFIS (AFIS) shall provide the capability to control the false reject rate, which is

defined as the percentage of in-sequence submissions sent for human FSC, of AFIS ASC via AFIS threshold settings.

SYS1998 IAFIS (AFIS) shall provide a false reject rate for ASC of less then 50% on a known test set of in-sequence conditions.

SYS1999 IAFIS (AFIS) shall provide the capability to control the false accept rate, which is defined as the percentage of out-of-sequence submissions sent to AFIS without human FSC, of AFIS ASC via AFIS threshold settings.

SYS2000 IAFIS (AFIS) shall provide a false accept rate for ASC of less than 2% on a known test set of out-of-sequence conditions.

The following accuracy requirements are specific to latent processing:

SYS2001 IAFIS (AFIS) shall provide latent search results that identify the correct candidate within the top ten positions of the candidate list at least 65 percent of the time.

SYS2002 IAFIS (AFIS) shall provide latent search results that identify the correct candidate in the top-ranked position of the candidate list at least 50 percent of the time.

SYS2003 IAFIS (AFIS) shall perform Latent Fingerprint searches of the Criminal Ten-Print Fingerprint Features Master File unless the file penetration of the search will exceed 30 percent of the file.

SYS2004 IAFIS (AFIS) shall perform Latent Fingerprint searches of the Criminal Ten-Print Fingerprint Features Master File with a file penetration exceeding 30 percent of the file when submitted by an authorized FBI System Administrator.

SYS2005 IAFIS (AFIS) shall produce for each ten-print fingerprint search against the ULF, on average, a maximum of one false candidate.

4.3 System Availability

System availability is the time when the application must be available for use. Required system availability is used in determining when maintenance may be performed.

IAFIS is considered to be unavailable when IAFIS is unable to satisfy the response time and workload requirements.

4.3.1 IAFIS Availability

4.3.1.1 System Availability

SYS2006 IAFIS shall provide functional support 24 hours a day, seven days a week.

SYS2007 IAFIS shall provide an operational availability of 99.8 percent when measured over a thirty day consecutive period.

EFCON will include high-availability servers. If one fails, or is taken out of service for maintenance or upgrade, the others will take over processing.

SYS2008 EFCON shall be available 24 hours/day 365 days/year.

NGI-462

SYS2274 IAFIS (iDSM) shall be available for shared data access by IDENT a minimum of 99% measured over a one month period.

4.4 Supportability/Maintainability

This section includes any operational requirement that enhances the supportability or maintainability of the system being built, including maintenance access, maintenance utilities, maintenance schedules, or architectural considerations required to provide for long term ease of maintenance.

4.4.1 Support Multiple System Environments

IAFIS must have the capability to concurrently support the system environments defined below:

- Operational: IAFIS operating in its normal configuration with complete data integrity and availability of all segments to normal users, service providers, and operators.
- Non-Operational Test: IAFIS providing segment and system test capabilities and operating with a separate subset of data that is unavailable to normal system users.
- Non-Operational Development: IAFIS providing segment development and maintenance and operating with a separate subset of data that is unavailable to normal system users.

SYS2009 IAFIS shall provide an Operational Environment.

SYS2010 IAFIS shall provide a Non-Operational Testing Environment(s).

SYS2011 IAFIS shall provide a Non-Operational Development Environment.

The test and development environment will support assessment of IAFIS operational effectiveness and operational suitability.

SYS2012 IAFIS shall support the capability for applications or data present in one environment to not impact applications or data from another environment.

SYS2013 IAFIS shall support the capability to operate multiple environments simultaneously.

SYS2014 IAFIS shall support a common System Administration functions with the same controls, tools, and utilities for the multiple environments.

SYS2015 IAFIS shall support the capability for the System Administrator to control access to all non-operational environments (i.e., development, test, and training).

SYS2016 IAFIS shall support System Administrator controls that adjust the boundaries among the environments.

SYS2017 IAFIS shall support System Administrator controls that allocate the amount of resources to each environment.

SYS2018 IAFIS shall support System Administrator controls that adjust segment priorities for each environment.

4.4.1.1 Operational Environment

SYS2019 IAFIS shall support the use of startup routines on the Operational Environment.

SYS2020 IAFIS shall support the use of shutdown routines on the Operational Environment.

SYS2021 IAFIS shall support software distribution and management on the Operational Environment.

SYS2022 IAFIS shall provide the capability for authorized users to retrieve a subset of the Operational databases to be used for populating the IAFIS Non-Operational Test environments.

SYS2023 IAFIS shall provide the capability for authorized users to retrieve a subset of the Operational databases to be used for populating the IAFIS Non-Operational Development environments.

SYS2024 IAFIS (ITN) shall provide the capability for the System Administrator to initiate workstation broadcast messages and notifications on the Operational Environment.

Workstation broadcast messages and notifications will interrupt workstation operations and be displayed at the workstation.

4.4.1.2 Non-Operational Test Environment

The IAFIS non-operational test environment supports testing of new or upgraded hardware, testing inter-segment interfaces, testing software upgrades in any segment, and end-to-end testing of IAFIS services.

SYS2025 IAFIS shall support a Non-Operational Test Environment that consists of a set of test data separate from the operational data.

SYS2026 IAFIS shall ensure that modifications to the Non-Operational Test environment do not affect the Operational environment.

SYS2027 IAFIS shall support the use of startup routines on the Non-Operational Test Environment.

SYS2028 IAFIS shall support the use of shutdown routines on the Non-Operational Test Environment.

SYS2029 IAFIS shall support software distribution and management on the Non-Operational Test Environment.

SYS2030 IAFIS shall provide the capability for the System Administrator to initiate workstation broadcast messages and notifications on the Non-Operational Test Environment.

SYS2031 IAFIS shall provide the capability for the Non-Operational test data to be restored to its initial state after testing is completed.

SYS2032 IAFIS shall provide the capability for the Non-Operational Test Environment to test the functionality and performance capabilities of the IAFIS Operational Environment.

SYS2033 IAFIS shall provide access for authorized operators, trainers, developers, and testers to the Non-Operational Test environments.

SYS2034 IAFIS shall ensure that the Non-Operational Test Environment does not impact the performance, availability, data confidentiality, or data integrity of the operational environment.

SYS2035 IAFIS shall have the capability to maintain test databases and files in the Non-Operational Test environment that parallel data used by the operational system.

SYS2036 IAFIS shall provide the capability to perform integration testing on the Non-Operational Test environment.

SYS2037 IAFIS shall provide the capability for the Non-Operational Test environment to support message generation and response capture for segment-level testing.

SYS2038 IAFIS shall support the operational IAFIS accuracy, workload, and scalable database capacities for each segment within IAFIS on the Non-Operational Test environment.

SYS2039 IAFIS shall maintain testing databases of synchronized test data (reflecting the same population of subjects) across all segments in the Non-Operational Test environment.

SYS2040 IAFIS shall provide the user interface and input/output capabilities as necessary to interact with the Non-Operational Test environment.

SYS2041 IAFIS shall provide the capability to back up and restore all test data (e.g., databases, files, tunable parameters) supporting the Non-Operational Test environment.

SYS2042 IAFIS shall provide the means to restore the default parameters at any time in the Non-Operational Test environment.

The following requirements are specific to provide NOE External User Testing using the Non-Operational Test environment:

SYS2043 IAFIS shall provide the capability for external users to submit test system transactions to the Non-Operational Test environment to ensure that their equipment is properly interconnected and that the system transaction is processed.

SYS2044 IAFIS shall provide the capability to restrict access of external testing system transactions to the set of IAFIS test files required to properly acknowledge the system transaction and generate the response on the Non-Operational Test environment.

SYS2045 IAFIS shall provide the capability for interactive instructional training exercises and scenarios on the Non-Operational Test Environment.

SYS2046 IAFIS shall provide the capability to simulate real-time IAFIS operations on the Non-Operational Test environment.

SYS2047 IAFIS shall provide the capability to respond to external testing system transactions that include rejections for invalid transaction formats, Identification and Non-Identification decisions, and criminal history requests on the Non-Operational Test environment.

External users should not need special telecommunications equipment to access the test mode. External users must coordinate access to test mode with an IAFIS System Administrator.

4.4.1.3 EFCON Test Environment

When a contributing agency on the CJIS WAN is bringing a new part of their system online or a new agency is joining the system, the contributor can verify IAFIS compliance for all EFTS transactions through an automated test system in the Operational Environment. The contributing agency submits a transaction for testing by sending it to the email address for the test node, rather than the usual EFCON address.

SYS2048 IAFIS (EFCON) shall provide an automated test system in the EFCON Operational Environment to verify IAFIS and EFTS message compliance.

SYS2049 IAFIS (EFCON) shall provide automated test system responses to agencies submitting test transactions.

The test system response will contain either an SRE (search results electronic), which means the transaction is 100 % compliant, or an ERRT (error transaction), which indicates some problems.

SYS2050 IAFIS (EFCON) shall include fields that are not in compliance in the test system error response.

SYS2051 IAFIS (EFCON) shall provide test system availability 24 hours/day, 365 days/year on the Operational Environment.

External users may send messages to the EFCON test environment during normal operational use of IAFIS to test connectivity at the message level, request that EFCON evaluate the format of their messages, and request that EFCON send them correctly formatted test response messages. Currently, CJIS does not permit external users to access the FBI test environments even though the hardware capability exists. The following statements would be applicable if external users were permitted to connect to the NOE test systems.

The following requirements are specific to an NOE EFCON Test System:

SYS2052 IAFIS (EFCON) shall provide test system availability 24 hours/day, 365 days/year on the Non-Operational Environment.

SYS2053 IAFIS (EFCON) shall provide the capability to duplicate the Operational system transactions on the Non-Operational Environment.

SYS2054 IAFIS (EFCON) shall send responses to EFCON test messages from external users in accordance with the EFTS.

SYS2055 IAFIS (EFCON) shall examine the format of external user test messages to determine their compliance with the IAFIS ICD.

SYS2056 IAFIS (EFCON) shall report the results of format examinations to the user.

SYS2057 IAFIS (EFCON) shall provide a capability for external users to select and receive test messages from a test message table.

SYS2058 IAFIS (EFCON) shall provide a capability for an authorized external user to connect with the IAFIS test support environment to perform system-level testing.

SYS2059 IAFIS (EFCON) shall provide the EFCON System Administrator the capability to control all external user access and connectivity to the EFCON test support environment.

SYS2060 IAFIS (EFCON) shall restrict external testing user's access to the EFCON test processes and test data.

SYS2061 IAFIS (EFCON) shall support EFCON IAFIS non-operational test environment for external user testing using the same type of telecommunications equipment as the operational system.

SYS2062 IAFIS (EFCON) shall provide a response to an external user test message within 30 seconds of receipt while processing the required average workloads and meeting all other required response times. NGI-466

4.4.1.4 Non-Operational Development Environment

SYS2063 IAFIS shall support the Non-Operational Development Environment for development, maintenance, and testing of IAFIS software and hardware that is separate from other IAFIS environments.

SYS2064 IAFIS shall support the Non-Operational Development Environment for development, maintenance, and testing of software and hardware.

SYS2065 IAFIS shall ensure that the Non-Operational Development Environment does not impact the performance, availability, data confidentiality, or data integrity of the Operational Environment.

SYS2066 IAFIS shall ensure that the III Non-Operational Development Environment is separate from other IAFIS Non-Operational Development Environments.

SYS2067 IAFIS shall ensure that the AFIS Non-Operational Development Environment is separate from other IAFIS Non-Operational Development Environments.

SYS2068 IAFIS shall ensure that the ITN Non-Operational Development Environment is separate from other IAFIS Non-Operational Development Environments.

SYS2069 IAFIS shall support authorized users with access privileges necessary to code and test software and new releases on the Non-Operational Development Environment.

Authorized users will have the ability to compile and link code developed on the Non-Operational Development Environment. Testing on the Non-Operational Development Environment will consist of unit testing, Computer Software Component (CSC) integration testing, and hardware and software Configuration Item (CI) integration testing.

SYS2070 IAFIS shall support a Non-Operational Development Environment that consists of a set of data separate from other environments.

SYS2071 IAFIS shall support the operational IAFIS accuracy and scalable database capacities for each segment within IAFIS on the Non-Operational Development environments.

4.5 System Performance

4.5.1 IAFIS User Service Response Times

SYS2072 IAFIS shall measure average response times over a seven day calendar week.

SYS2073 IAFIS shall satisfy the system response times when presented with system transaction workloads of up to 130% of the values presented in Table 4.7.1-1.

SYS2074 IAFIS shall measure system response time from the receipt of the complete system transaction until the initiation of the electronic response transmission or printing of the hardcopy reply.

SYS2075 IAFIS (III) shall provide the capability to sustain response time requirements for at least one hour under a workload of 4 times that specified in Table 4.6.1-1.

4.5.1.1 Identification Services Response Times

SYS2076 IAFIS (ITN) shall complete processing of 99 percent of all Ten-Print two hour response time transactions within three hours.

SYS2077 IAFIS (ITN) shall complete processing of 99 percent of all Ten-Print 24 hour response time transactions within 48 hours.

SYS2078 IAFIS (III) shall respond to Ten-print Submission subject search request of the criminal database within 15 seconds 98% of the time.

SYS2079 IAFIS shall satisfy the response times for Criminal Ten-Print Identification submissions as specified in Table 4.5.1-1.

Table 4.5.1-1 Average System Transaction Processing Times for Criminal Ten-Print Submissions

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Criminal Ten-Print Urgent Submissions					
Electronic Submissions	2h	1m	1h 39m	5m	15m max
Hard-Copy Submissions	2h	NA	1h 39m	5m	15m max
Remote Searches	2h	1m	31m	5m	1h 23m
Criminal Ten-Print Non-Urgent Submissions					
Electronic Submissions	24h	1m	23h 24m	5m	30m
Hard-Copy Submissions	24h	NA	23h 25m	5m	30m
Electronic Latent Submissions (LFS)	24h	1m	1m	N/A	23h 58m
Hard-Copy Latent Submissions (ILFS)	24h	N/A	1m	N/A	23h 59m
CSS Submissions	30d	1m	29d 23h 24m	5m	30m
Remote Searches	24h	1m	31m	5m	23h 23m

Legend: h=hours; m=minutes; ms=milliseconds; s=seconds; max=maximum processing time

** Includes IAFIS Backbone and ITN Communications.

SYS2080 IAFIS (III) shall respond to an Identification Subject Search request of the civil database in less than ten seconds 98% of the time.

SYS2081 IAFIS shall satisfy the response times for Civil Ten-Print Identification submissions as specified in Table 4.5.1-2.

Table 4.5.1-2 Average System Transaction Processing Times for Civil Ten-Print Submissions

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Civil Ten-Print Urgent Submission					
Electronic Submissions	15m				
Civil Ten-Print Non-Urgent Submissions					

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Electronic Submissions	24h	1m	23h 24m	5m	30m
CSS Submissions	30d	1m	29d 23h 24m	5m	30m
Hard-copy Submissions	24h	NA	23h 25m	5m	30m
Remote Searches	24h	1m	31m	5m	23h 23m
Humanitarian Submissions	24h	N/A	22h 50m	10m	1h

Legend: h=hours; m=minutes; ms=milliseconds; s=seconds; max=maximum processing time

** Includes IAFIS Backbone and ITN Communications.

4.5.1.2 Information Services Response Times

SYS2082 IAFIS (III) shall sustain Subject History Retrieval response times for at least one hour under a workload of 4 times that specified in Table 4.7.1-1.

SYS2083 IAFIS (III) shall perform Filter Requests with one FBI Number within ten seconds 98% of the time.

SYS2084 IAFIS (III) shall perform Filter Requests with up to 100 FBI Numbers within 150 seconds 98% of the time.

SYS2085 IAFIS (III) shall perform Filter Requests with up to 100 FBI Numbers within 180 seconds all of the time.

SYS2086 IAFIS (III) shall sustain Filter Request response time requirements for at least one hour under a workload of that specified in Table 4.7.1-1.

SYS2087 IAFIS (III) shall process 5,000 FBI Number checks per hour.

For example, a likely scenario is 500 Filter Requests per hour with 10 FBI Numbers in each request for a total of 5,000 FBI Number checks.

SYS2088 IAFIS (III) shall perform Criminal Photo Retrieve Requests within 30 minutes all of the time when photo exists.

SYS2089 IAFIS (III) shall perform Criminal Photo Retrieve Requests within 2.8 seconds 95% of the time when photo does not exist.

SYS2090 IAFIS (III) shall perform Criminal Photo Retrieve Requests within 10 seconds all of the time when the photo does not exist.

SYS2091 IAFIS (III) shall perform Criminal Photo Add Requests within 2.8 seconds 95% of the time.

SYS2092 IAFIS (III) shall perform Criminal Photo Add Requests within 10 seconds all of the time.

SYS2093 IAFIS (III) shall perform Criminal Photo Delete Requests within 20 seconds all of the time.

SYS2094 IAFIS (ITN) shall provide a response to a certification file request within 3 hours from the time of receipt.

SYS2095 IAFIS shall satisfy the response times for Information Services as specified in Table 4.5.1-3.

Table 4.5.1-3 Average System Transaction Processing Times for Information Services

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Image Request Services					
Known Fingerprint Image Requests	24h	1m	23h 54m	5m	N/A
Interstate Photo System (IPS) Services					
Criminal Photo (mug shot) requests	30m 2s	100ms	100ms	30m	NA
Criminal Photo Not Found Response	3s	100ms	100ms	2.8s	NA
Criminal Photo (mug shot) Delete request	20.1s	100ms	N/A	20s	N/A
Filter Request* (Single FBI Number)				20s	

Legend: h=hours; m=minutes; ms=milliseconds; s=seconds; max=maximum processing time

** Includes IAFIS Backbone and ITN Communications.

4.5.1.3 Investigative Services Response Times

SYS2096 IAFIS shall provide a response to a Ten-Print Fingerprint Rap Sheet search request within 3 minutes of receipt.

SYS2097 IAFIS shall provide a response to a Ten-Print Fingerprint Rap Sheet search request within 2 minutes 90% of the time.

SYS2098 IAFIS (III) shall respond to all other electronic subject search requests within 2.8 seconds 98% of the time, for any search with less than 350 candidates.

SYS2099 IAFIS (III) shall respond to all other electronic subject search requests within ten seconds all of the time, for any search with less than 350 candidates.

SYS2100 IAFIS (III) shall respond to an Investigative Subject Search request of the civil database in less than ten seconds 98% of the time.

SYS2101 IAFIS shall satisfy the response times for Latent Investigative submissions as specified in Table 4.5.1-4.

Table 4.5.1-4 Average System Transaction Processing Times for Latent Investigative Submissions

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Latent Print Services					
Latent Remote Searches (LFIS/LFFS)	24h	1m	31m	5m	23h 23m
Cascaded ULF Searches	24h	N/A	1h	5m	22h 55m
Internal Unsolved Latent Searches (IULS/IULTS)	40m	N/A	30m	N/A	10m
Internal Unsolved Latent Records Delete (IULD)	31m	N/A	30m	N/A	1m
Remote Unsolved Latent Record Delete (ULD)	33m	1m	30m	1m	1m

NGI-470

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
ULF Maintenance (Add)	2m	N/A	1m	N/A	1m
Special Latent Cognizant Search (Latent and Ten-Print) 50,000 records*** (NDR=SLCN)	37m	N/A	32m	N/A	5m
Special Latent Cognizant Search (Latent and Ten-Print) 500,000 records*** (NDR=SLCN)	1h32m	N/A	32m	N/A	1h
Latent Penetration Query (External LPNQ)	7m	1m	N/A	5m	1m
Latent Penetration Query (Internal ILPNQ)	1m30s	N/A	30s	N/A	1m
Latent Repository Statistics Query (External LRSQ)	7m	1m	N/A	5m	1m
Latent Search Status and Modification Query (External LSMQ)	7m	1m	N/A	5m	1m
Latent Search Status and Modification Query (Internal ILSMQ)	1m30s	N/A	30s	N/A	1m
Major Case Print (MCS)			30m		

Legend: h=hours; m=minutes; ms=milliseconds; s=seconds; max=maximum processing time

** Includes IAFIS Backbone and ITN Communications.

*** Search time includes image retrieval for candidate images, but not network transmission time to/from remote other Federal organization workstations.

SYS2102 IAFIS (III) shall perform Criminal Database Ad Hoc Subject Searches within 30 hours 95% of the time.

SYS2103 IAFIS (III) shall sustain the ad hoc subject search response time under a workload of four times that specified in Table 4.7.1-1 for at least two days.

SYS2104 IAFIS (III) shall perform Civil Database Ad Hoc Subject Searches within 30 hours 95% of the time.

SYS2105 IAFIS (III) shall sustain the Civil Database ad hoc subject search response time under a workload of four times the size specified in Table 4.7.1-1 for at least two days.

SYS2106 IAFIS shall satisfy the response times for Subject Search & Subject History Request Services as specified in Table 4.5.1-5.

Table 4.5.1-5 Average System Transaction Processing Times for Subject Search & Subject History Request Services

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Subject Search & Subject History Request Services					
Subject Searches* (Criminal)	3.7s	900ms	N/A	2.8s	NA
Subject Searches (MRD)	24h				
Ad Hoc Queries (Criminal or Civil)	24h	N/A NGI-471	1m	23h 59m	NA

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Subject History Retrieval Requests* (Criminal or Civil)	3.7s	900ms	N/A	2.8s	NA

Legend: h=hours; m=minutes; ms=milliseconds; s=seconds; max=maximum processing time

* Times in these system transactions rows are maximum values, not averages.

** Includes IAFIS Backbone and ITN Communications.

4.5.1.4 Data Management Services Response Times

SYS2107 IAFIS shall provide a response to a Computerized Contributor Address File maintenance request within 15 seconds of receipt.

SYS2108 IAFIS (III) shall perform the Subject History File Maintenance add request within 2.8 seconds 98% of the time.

SYS2109 IAFIS (III) shall provide the capability to sustain Subject History File Maintenance add response time requirements for at least one hour under a workload of 4 times that specified in Table 4.7.1-1.

SYS2110 IAFIS (III) shall perform Subject History Maintenance update requests within 5 seconds 95% of the time.

SYS2111 IAFIS (III) shall sustain Subject History Maintenance update response times for at least one hour under a workload of 4 times that specified in Table 4.7.1-1.

SYS2112 IAFIS (III) shall perform the Computerized Contributor Address (CCA) File add request within 5 seconds 98% of the time.

SYS2113 IAFIS (III) shall perform the Subject History Maintenance delete request of a single record within 10 seconds 98% of the time.

SYS2114 IAFIS (III) shall perform a Subject History Maintenance request to delete a single record within 45 seconds all of the time.

SYS2115 IAFIS (III) shall sustain Subject History Maintenance delete response times for at least one hour under a workload of 4 times that specified in Table 4.7.1-1.

SYS2116 IAFIS (III) shall perform Subject History File Consolidation requests within 20 seconds 98% of the time.

SYS2117 IAFIS (III) shall sustain Subject History File Consolidation response times for at least one hour under a workload of 4 times that specified in Table 4.7.1-1.

SYS2118 IAFIS (ITN) shall perform a certification file add request within 5 minutes from the time of receipt.

SYS2119 IAFIS shall satisfy the response times for Document Submission Services (e.g., dispositions, expungements) as specified in Table 4.5.1-6.

Table 4.5.1-6 Average System Transaction Processing Times for Document Submission Services

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
Document Submission Services					

NGI-472

System Transaction Type	IAFIS System	ITN IAFIS FE	ITN PROC**	III	AFIS
MRD	24h	NA	5m	23h 55m	NA
Hard-Copy	24h	NA	23h 55m	5m	NA
Subject History File Maintenance* (Criminal or Civil)	10s	NA	NA	10s	NA
Subject History File Consolidation*				60s	
Want Update Notification from NCIC 2000 ($.A.WPT)	1.8s	900ms	N/A	900ms	N/A
ORI File Update ($.A.ORI) and Line File Update ($.A.LIN) Message Processing	2m	1m		1m	

Legend: h=hours; m=minutes; ms=milliseconds; s=seconds; max=maximum processing time

** Includes IAFIS Backbone and ITN Communications.

4.5.2 Image Storage and Retrieval Response Times

SYS2120 IAFIS (ITN/ISRE) shall process image copy requests within 48 hours.

SYS2121 IAFIS (ITN/ISRE) shall process the hourly fingerprint image retrieval requests as shown Table 4.5.2-1 FY 2008 Hourly FIMF Retrievals 15 Minute Response Time.

SYS2122 IAFIS (ITN/ISRE) shall perform hourly FIMF retrieval requests within 30 minutes 98 percent of the time.

SYS2123 IAFIS (ITN/ISRE) shall perform hourly FIMF retrieval requests within 5 minutes 2 percent of the time.

SYS2124 IAFIS (ITN/ISRE) shall process Unsolved Latent Fingerprint Image File image retrieval requests within 30 minutes.

SYS2125 IAFIS (ITN/ISRE) shall process Latent Photo File image additions and retrieval requests within 30 minutes.

SYS2126 IAFIS (ITN/ISRE) shall process SLC Ten-print Image File transactions within 30 minutes.

SYS2127 IAFIS (ITN/ISRE) shall be capable of performing up to 150 percent of the required average workloads while still satisfying the response time requirements.

Table 4.5.2-1 FY 2008 Hourly FIMF Retrievals 15 Minute Response Time

Hour	Subject Search Candidates	Ten-print Search Candidates	Total	Percent
0000-0059	20	50	70	3%
0100-0159	20	50	70	3%
0200-0259	20	50	70	3%
0300-0359	20	40	60	2%
0400-0459	20	30	50	2%
0500-0559	20	40	60	2%
0600-0659	10	30	40	2%
0700-0759	20	40	60	2%

0800-0859	30	70	100	4%
0900-0959	40	110	150	6%
1000-1059	50	130	180	7%
1100-1159	50	130	180	7%
1200-1259	50	120	170	6%
1300-1359	50	120	170	6%
1400-1459	50	130	180	7%
1500-1559	50	130	180	7%
1600-1659	50	120	170	6%
1700-1759	40	100	140	5%
1800-1859	30	70	100	4%
1900-1959	30	70	100	4%
2000-2059	30	60	90	3%
2100-2159	30	60	90	3%
2200-2259	20	60	80	3%
2300-2359	20	50	70	3%
Daily Totals	770	1860	2630	100%

4.5.3 User Fee Billing Response Times

The User Fee Billing response times do not take into account response time estimates for manual intervention.

SYS2128 IAFIS (IDWH) shall provide On-line User Fee Billing response times in accordance with Table 4.5.3-1, UFBS On-Line Data Response Time Requirements.

SYS2129 IAFIS (IDWH) shall provide On-Line and Off-Line sustainable response times to be under load for one hour.

Table 4.5.3-1 UFBS On-Line Data Response Time Requirements

Type of Request	Response Time (95%)	Response Time (max)
Report Request		
Automatic Report Request (request to retrieve a report which is automatically generated at regular intervals and stored on-line)	1 min	15 min
On-Demand Report Generation Requests (request to generate a pre-defined report)	2 min	30 min
On-Demand Report w/Requestor Range Specifications Generation Request (request generation of a pre-defined report with requestor specified modification to field ranges such as date ranges)	2 min	30 min
Ad Hoc Report Generation Request (request generation of report based on requestor defined report format and data layouts.)	5 min	45 min
Individual User Fee Bill Request	2 min	30 min
Database Management		
Update Request	5 min	30 min
Add Request	5 min	30 min
Delete Request	5 min	30 min
Ad Hoc Queries		
Simple Query of User Fee Data (simple query uses any or all of the following parameters: ICN, Type of Transaction, ORI, Reject Code, Subject/Applicant Name, CIDN, CRI, OCA, Time/Date Range)	1 min	15 min
Complex Query of User Fee Data (complex query uses more parameters than those defined for simple query)	2 min	30 min
Pre-Defined Queries	30 sec	5 min
Data Loading	2 hr	6 hr

NGI-474

Type of Request	Response Time (95%)	Response Time (max)
Archive (move off-line) Data Request	2 hr	6 hr

SYS2130 IAFIS (IDWH) shall provide On-line User Fee Billing response times in accordance with Table 4.5.3-2, UFBS Off-Line Data Response Time Requirements.

Table 4.5.3-2 UFBS Off-Line Data Response Time Requirements Requirements

Type of Request	Response Time (95%)	Response Time (max)
Report Request		
Automatic Report Request (request to retrieve a report which is automatically generated at regular intervals and stored on-line)	N/A	N/A
On-Demand Report Generation Requests (request to generate a pre-defined report)	30 min	6 hr
On-Demand Report w/Requestor Range Specifications Generation Request (request generation of a pre-defined report with requestor specified modification to field ranges such as date ranges)	30 min	6 hr
Ad Hoc Report Generation Request (request generation of report based on requestor defined report format and data layouts.)	1 hr	6 hr
Individual User Fee Bill Request	30 min	6 hr
Database Management (using data retrieved off-line)		
Update Request	2 hr	8 hr
Add Request	2 hr	8 hr
Ad Hoc Queries		
Simple Query of User Fee Data (simple query uses any or all of the following parameters: ICN, Type of Transaction, ORI, Reject Code, Subject/Applicant Name, CIDN, CRI, OCA, Time/Date Range)	1 hr	6 hr
Complex Query of User Fee Data (complex query uses more parameters than those defined for simple query)	2 hr	6 hr
Pre-Defined Queries	30 min	6 hr

4.5.4 Shared Data Response Times

SYS2275 IAFIS (iDSM) shall respond to a criminal Ten-Print Fingerprint Identification Search of the IDENT shared data records within two hours after receipt by iDSM.

SYS2276 IAFIS (iDSM) shall respond to a civil Ten-Print Fingerprint Identification Search of the IDENT shared data records within twenty four hours after receipt by iDSM.

SYS2277 IAFIS (iDSM) shall provide a response to a shared data search within the required time allotment 95% of the time measured over a month for the end-user, not including the LESC response time.

SYS2278 IAFIS (iDSM) shall provide the results of the shared data post processing (QA) on all positive identifications against the IDENT shared data records within 24 hours.

4.5.5 Workstation Response Times

SYS2131 IAFIS (ITN) shall provide the response times for automatic workstation functions shown in Table 4.5.4-1.

Table 4.5.4-1 Workstation Function Time Specifications

Function	Function Time Specification
Display of entire Human-Machine Interface Screen (updated and ready for user interaction)	1 second from time of request
Access and display of first image during start or change of functions	10 seconds from time of request*
Response to Enter Key or Completion of a Data Entry Screen	1 second
* Not to exceed 10 seconds under full operational load which may include compression/decompression, network access, or storage media access as required.	

4.6 IAFIS Capacity

4.6.1 IAFIS Overall

SYS2132 IAFIS shall support the yearly storage capacity requirements as specified in table 4.6.1-1.

Table 4.6.1-1 File Size in Millions By Year

	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008
Civil Subject Index Master File (records)	3.720	4.524	5.348	6.192	7.056	7.940	8.844	9.768	10.712	11.676
Subject Criminal History File (subjects)	40.480	42.977	45.491	48.019	50.564	53.124	55.699	58.290	60.896	63.516
On-line CRS File	7,164	7,107	6,811	6,511	6,207	5,898	5,585	5,267	4,944	4,617

SYS2133 IAFIS (ITN/AFIS) shall have the ability to logically create at least 35 separate files with a maximum of 500,000 records in any one file.

The maximum number of records for all SLC files is 1.5 million. The maximum number of files allotted to LFPS is 25 files. The maximum number allotted to OFO is one per agency (initially anticipating up to 10 agencies). The initial allotment of records for LFPS is 500,000. The initial allotment of records for OFO is 100,000 records per file, with a maximum total of 1 million records.

SYS2134 IAFIS (III) shall support up to 150,000 Computerized Contributor Address File records.

SYS2135 IAFIS (ITN/LPS) shall provide storage for 6,000 latent search requests.

SYS2136 IAFIS (EFCON) shall provide a tape library with 20 terabytes of capacity to support data archiving, backup, and recovery. NGI-476

SYS2137 IAFIS (ITN/ISRE) shall support a MCP repository of 15,700 records in the year 2005

and 25,000 records in the year 2008.

The size of a compressed Major Case Print File record is 6 MB (15:1 Compression).

SYS2138 IAFIS (ITN/ISRE) shall support a MCP size of 100 GB in the year 2005 and 150 GB in the year 2008.

SYS2139 IAFIS (ITN/ISRE) shall support the image storage capacity requirements for the year 2000 and 2008 shown in Table 4.6.1-2.

Table 4.6.1-2 ISRE Storage Capacity Requirements

File	Records (Year 2000)	Records (Year 2008)
FIMF	42,977,000	63,518,000
Civil Ten-print On-Line File	4,524,000	11,676,000
Unsolved Latent Fingerprint Image File	250,000	250,000
Latent Photo File	500,000	500,000
Special Latent Cognizant Ten-print Image File	1,500,000	1,500,000
Test Image Files	400,000	400,000

SYS2140 IAFIS (III/IPS) shall support a Criminal Subject Photo File of up to 6,000,000 records.

4.7 Workload

4.7.1 Support IAFIS Workload

The workload is the total number of messages to be delivered by IAFIS/BCE while meeting all required response time requirements without loss of data or messages.

SYS2141 IAFIS shall be sized to support the peak hour traffic of system messages at any time during the day.

SYS2142 IAFIS shall support the peak hour traffic without performance degradation.

SYS2143 IAFIS shall support peak minute traffic, which occurs once during the peak hour and is 4.0 percent of the peak hour traffic.

SYS2144 IAFIS shall be able to support the simultaneous occurrence of peak minute traffic for all messages.

SYS2145 IAFIS shall be able to support the daily transaction workloads which are specified in Table 4.7.1-1.

Table 4.7.1-1 Daily System Transaction Fiscal Year 2008 Projected Workload

System Transaction Type	Daily System Transaction Workload
NGI-477 Ten-Print Services	

System Transaction Type	Daily System Transaction Workload
Criminal Submissions	49,100
requiring only subject search	35,300
requiring feature-based processing	13,800
Civil Submissions	47,600
requiring only criminal subject search	10,600
requiring criminal feature-based processing	37,000
Civil file daily addition from Civil Submissions	12,300
Remote Ten-print Requests	54,000
Urgent Remote Searches Rap Sheet Return	49,000
Non-urgent Remote searches	5,000
Unknown Deceased, Missing, Amnesia, Victim, Living John Doe	
With FP cards requiring criminal search and civil search	15
Civil File Processing Request (from Latent and FBI Service Providers)	
Subject Search (Name Request)	170
Military Name Changes	60
Request for Civil Master	200
Latent Print Services	
Latent Submissions	676
Latent Remote Searches	255
Unsolved Latent Add Requests	931
Unsolved Latent Delete Requests	931
LFPS-directed ULF Ten-Print Searches	50
LFPS-directed ULF Latent Searches	50
Latent Search of Special Latent File(s) 50,000 records	600
Latent Search of Special Latent File(s) 500,000 records	100
Ten-print Search of Special Latent File(s) 50,000 records	40
Ten-print Search of Special Latent File(s) 500,000 records	10
Create Logical Special Latent File	1
Delete Logical Special Latent File	1
Add new records to Special Latent File	3,000
Add existing IAFIS records to Special Latent File	80,000
Delete Special Latent File record	3,000
Subject Search & Criminal History Request Services	
Subject Searches (Includes Search from Ten-Print and Document Submissions)	992,000
Ad Hoc Queries—Criminal Subject History File	100
Ad Hoc Queries—Civil Subject Index Master File	50
Criminal History Requests	114,000
Document Submission Services	

NGI-478

System Transaction Type	Daily System Transaction Workload
Consolidation Requests	135
Death Notices	10
Disposition Reports	26,400
Expungement Requests	2,635
Record Sealing Requests	10
Federal Agency Subject Searches	80
Freedom of Information Act Requests	450
Miscellaneous Document Processing	1,400
Remote Fingerprint Image Services	
Fingerprint Image Requests	2,500
Criminal Photo Image Services	
Criminal Photo Image Requests	250
Criminal Photo Image Delete Requests	15
Want and Flash Notifications	20,000
Want and Flash Discrepancy Resolution Messages	200
Notify Originator of Want and Flash	2,700
Sexual Offender Registry Notifications	2,000
Sexual Offender Registry Discrepancy Resolution Messages	100
Notify Originator of Sexual Offender Registry	200
Purge of Pre-trial Diversion Flash Data	175 per month, once a month
ORI File Update ($.A.ORI) messages form NCIC 2000	100
Line File Update ($.A.LIN) messages from NCIC 2000	15
Computerized Contributor Address (CCA) File Ad Hoc Search	50
Computerized Record Sent (CRS) File Retrieval	200

SYS2146 IAFIS (EFCON) shall process up to 169,000 transactions per day, including CSS transactions.

SYS2147 IAFIS (EFCON) shall process up to 169,000 responses from IAFIS.

SYS2148 IAFIS (EFCON) shall provide the capability of processing transactions at a peak capacity of 8,900 per hour.

SYS2149 IAFIS (EFCON) shall provide the capability of processing responses at a peak capacity of 8,900 per hour.

NGI-479

SYS2150 IAFIS (EFCON) shall have an average transaction delay of no more than 15 seconds over any one hour period.

SYS2151 IAFIS (ITN/TPS) shall provide the storage capacity for 5 work days of electronic submissions.

SYS2152 IAFIS (ITN/TPS) shall provide storage capacity for 5 days of inter-segment and intra-segment transactions.

SYS2153 IAFIS (ITN) shall support the processing of the average hourly ten-print submission and distribution rates for Fiscal Year (FY) 2008 as shown in Table 4.7.1-2 and Table 4.7.1-3.

Table 4.7.1-2 FY 2008 Hourly Arrivals to Ten-Print Processing

Hour	Criminal		Civil		Urgent		
	Card (CSS)	Electronic	Card (CSS)	Electronic	MRD	Card (CSS)	Electronic
0000-0059	0	250	0	270	0	0	30
0100-0159	0	250	0	270	0	0	30
0200-0259	0	230	0	250	0	0	30
0300-0359	0	180	0	200	0	0	20
0400-0459	0	150	0	160	0	0	20
0500-0559	0	170	0	180	0	0	20
0600-0659	0	140	0	150	0	0	20
0700-0759	0	170	0	180	0	0	20
0800-0859	1440	330	1210	360	230	40	40
0900-0959	1440	550	1210	590	230	40	60
1000-1059	1440	680	1210	730	230	40	80
1100-1159	1440	700	1210	750	230	40	80
1200-1259	1440	640	1210	680	230	40	70
1300-1359	1440	620	1210	660	230	40	70
1400-1459	1440	700	1210	750	230	40	80
1500-1559	1440	670	1210	720	230	40	70
1600-1659	720	610	600	660	110	20	70
1700-1759	720	500	600	530	110	20	60
1800-1859	720	380	600	400	110	20	40
1900-1959	720	350	600	380	110	20	40
2000-2059	720	300	600	320	110	20	30
2100-2159	720	300	600	320	110	20	30
2200-2259	720	390	600	310	110	20	30
2300-2359	720	250	600	270	110	20	30
Totals	**17280**	**9410**	**14480**	**10090**	**2720**	**480**	**1070**

Table 4.7.1-3 FY 2008 Hourly Distribution of Workload to Ten-Print Processing

Hour	Fingerprint Sequence Check	Fingerprint Image Compare
0000-0059	70	120
0100-0159	70	120
0200-0259	70	120
0300-0359	70	120
0400-0459	70	120
0500-0559	70	120
0600-0659	1560 NGI-480	2490

Hour	Fingerprint Sequence Check	Fingerprint Image Compare
0700-0759	4510	7210
0800-0859	4730	7560
0900-0959	3110	4980
1000-1059	4250	6790
1100-1159	2690	4310
1200-1259	3610	5770
1300-1359	4610	7380
1400-1459	3800	6070
1500-1559	670	1070
1600-1659	1980	3160
1700-1759	2090	3350
1800-1859	890	1410
1900-1959	2640	4220
2000-2059	2090	3340
2100-2159	2690	4310
2200-2259	2380	3810
2300-2359	3080	4930
Totals	**51800**	**82900**

SYS2279 IAFIS (iDSM) shall enroll shared data from III at least once a day.

SYS2280 IAFIS (iDSM) shall accept shared data enrollment requests from IDENT at least once a day.

SYS2281 IAFIS (iDSM) shall be capable of processing 1,000 shared data demotions from III per day.

SYS2282 IAFIS (iDSM) shall be capable of processing 1,000 shared data removals from III per day.

SYS2283 IAFIS (iDSM) shall be capable of processing 2,500 shared data enrollments from III per day.

SYS2284 IAFIS (iDSM) shall be capable of extracting feature vectors from IDENT shared data at a rate of 25 per day.

SYS2285 IAFIS (iDSM) shall be capable of supporting updates to the IDENT shared data at a rate of 200 changes per day.

SYS2286 IAFIS (iDSM) shall support a configurable number of IAQ searches per day.

Currently, IAFIS limits the number of IAQs to LESC to 80 requests per day.

SYS2287 IAFIS (iDSM) shall be capable of conducting up to 1,000 IAFIS Ten-Print Identification searches per day against the IDENT shared data records.

SYS2288 IAFIS (iDSM) shall be capable of performing 1,000 manual image comparisons of IAFIS Ten-Print submissions against the IDENT shared data records per day.

SYS2289 IAFIS (iDSM) shall have the storage capacity for 1,000,000 shared data records from IAFIS.

SYS2290 IAFIS (iDSM) shall have the storage capacity for 13 million IAFIS shared data Activity Log entries over five years.

NGI-481

SYS2291 IAFIS (iDSM) shall have the storage capacity for 1,000,000 shared data records from IDENT.

4.7.2 Support Special Latent Cognizant Processing Workload

Support OFO/SLC Searches

SYS2154 IAFIS (AFIS) shall process the daily workload of latent searches (that penetrate 30% of the latent cognizant file) as listed in the totals column of Table 4.7.2-1.

SYS2155 IAFIS (AFIS) shall allocate latent searches to state and federal users based upon the number of allocated searches in Allocation of Latent Searches in Table 4.7.2-1.

SYS2156 IAFIS (AFIS) shall provide the capability for the System Administrator to adjust the total number of searches and the number of searches for each individual organization.

Table 4.7.2-1 Allocation of Latent Fingerprint Searches *

State	Daily Allocation	Maximum Queued (5 x daily)	Total Searches	State	Daily Allocation	Maximum Queued (5 x daily)	Total Searches
Alabama	7	5	35	Montana	4	5	20
Alaska	4	5	20	Nebraska	12	5	60
Arizona	6	5	30	Nevada	4	5	20
Arkansas	5	5	25	New Hampshire	5	5	25
California	60	5	300	New Jersey	8	5	40
Colorado	5	5	25	New Mexico	5	5	25
Connecticut	5	5	25	New York	60	5	300
Delaware	4	5	20	North Carolina	14	5	70
District of Columbia	24	5	120	North Dakota	4	5	20
Florida	44	5	220	Ohio	12	5	60
Georgia	10	5	50	Oklahoma	6	5	30
Hawaii	4	5	20	Oregon	5	5	25
Idaho	4	5	20	Pennsylvania	23	5	115
Illinois	20	5	100	Rhode Island	4	5	20
Indiana	6	5	30	South Carolina	8	5	40
Iowa	5	5	25	South Dakota	4	5	20
Kansas	5	5	25	Tennessee	15	5	75
Kentucky	8	5	40	Texas	65	5	325
Louisiana	10	5	50	Utah	4	5	20
Maine	8	5	40	Vermont	4	5	20
Maryland	12	5	60	Virginia	20	5	3
Massachusetts	11	5	55	Washington	6	5	100
Michigan	12	5	60	West Virginia	29	5	145
Minnesota	4	5	20	Wisconsin	6	5	30
Mississippi	10	5	50	Wyoming	4	5	20
Missouri	4	5	20	**Total State**	634	5	3170
				FBI	218	5	1090
				OFO	200	5	1000
				Total	1052	5	5260

* Rules by which AFIS deals with LTTP allocations:

1. AFIS uses the CRI of the LTTP search to determine which Agency Type (State, OFO, or FBI) to use. This agency type determines which allocation will be "charged".

2. AFIS uses the following rules to determine Agency type:

a) Any ORI/CRI that matches the first 5 characters will be treated as the resulting Agency type as indicated below:

DCFBIxxxx → FBI
DCATFxxxx → OFO
MDNCAxxxx → OFO
VAUSAxxxx → OFO
VAUSMxxxx → OFO
VAPO0xxxx → OFO
DCSS1xxxx → OFO
DCDEAxxxx → OFO
GACIDxxxx → OFO
MDATFxxxx → OFO
DCPPDxxxx → OFO
WVFBIxxxx → FBI

b) USFBI is always charged to the FBI allocation space.

c) Usxxxxxxx (not USFBI) is charged to OFO.

d) If none of the above rules apply, it is a state ORI. The first two characters are used to determine which state allocation to "charge", (e.g., Alxxxxxxx → AL, WVxxxxxxx → WV)

3. AFIS allows 5 times the daily allocation of any Agency (including FBI and OFO) to be queued in the 5-day-LTTP queue on the Segcntrl machine.

4. Once a minute, the AFIS SCLT software batches latent searches, removes them from the 5-day-LTTP queue, and sends the batch to the processing servers.

5. Once a search is forwarded to the processing servers in a batch, it no longer takes up space on the queue. This then allows additional searches from that Agency to be submitted, EVEN THOUGH the total allocation is used up for that day.

6. If AFIS has the spare capacity to launch more searches from an Agency that has already used up its daily allocation, it will do so, WITHOUT waiting until the next day.

7. Once an Agency has filled up the 5-day-LTTP queue with 5 times its daily allocation, additional LTTP submissions will be rejected with an L0018 error code. If the Agency has a small allocation limit, then this may happen quickly. For example, WV (by default) has only 3 searches per day. After submitting 15 searches (assuming they remain in the queue), subsequent searches will be rejected. Usually the batching process empties/drains the queue before this can happen.

SYS2157 IAFIS (EFCON) shall accept and deliver the message traffic workload from external systems to the IAFIS segments in accordance with Table 4.7.2-2.

Table 4.7.2-2 EFCON Daily Message Traffic From External Systems

Messages From External Systems	Type	AFIS	III	ITN
NCIC FE				
Subject Search Requests	A		950,000	
Criminal History Requests	A		80,300	
Criminal Photo Delete Requests	A		500	
Criminal Photo Requests	A		9,000	
Special Organization Requests	U		100	
File Maintenance Requests	A		550	
Ad Hoc Query Request	A		100	
Dispositions	A		9,000	
Want and Flash Update Notification	A		14,900	
ORI File Update ($.A.ORI) and Line File Update ($.A.LIN) messages	A			1,500 (III)
Links to State CSAs and CSS				
Ten-print Fingerprint Search	B	22,000		
Ten-print Fingerprint Transaction (no Criminal Photo)	B NG			37,580

Messages From External Systems	Type	AFIS	III	ITN
Ten-print Fingerprint Transaction (with Criminal Photo)	G			5,000
Ten-print Fingerprint Transaction (CSS criminal w/ text image))	H			20,080
Ten-print Fingerprint Image Req.	A			16,000
Remote Latent Fingerprint Search	B	200		
Latent Fingerprint Transactions	B			200
Unsolved Latent Add Confirm	A			70
Unsolved Latent Fingerprint Delete	A			35
Penetration Query	A	3,175		
Repository Statistics Query	A	10		
Search Status and Modification Query	A	1,065		
	NIets			
			0	

4.8 System Characteristics

SYS2158 IAFIS shall adhere to the current CJIS Data Center and Facility Management policies when defining the environment in which IAFIS is located.

This Page Left Intentionally Blank.

BIBLIOGRAPHY

1. 40 U.S. Code 759, Computer Security Act of 1987, (Public Law 100-235), January 8, 1988.

2. 5 U.S. Code 552a, Privacy Act of 1974, (Public Law 93-579), December 1974.

3. American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, ANSI/NIST-ITL 1-2000, NIST Special Publication 500-245, September 2000.

4. American National Standards Institute (1988), *American National Standard for Forensic Identification - Automated Fingerprint Identification Systems - Glossary of Terms and Acronyms*, ANSI/IAI 2-1988, New York, NY.

5. Assistant Secretary of Defense (1985), *Department of Defense Trusted Computer System Evaluation Criteria*, (TCSEC), DOD 5200.28 STD, Washington, DC.

6. Criminal Justice Information Services (CJIS) Electronic Fingerprint Transmission Specification (EFTS), IAFIS-DOC-01078-7.1, V7.1, May 2, 2005.

7. Criminal Justice Information Services Controlled Access Protection Profile (CJISCAPP), Department of Justice, Federal Bureau of Investigation, December 8, 2003.

8. Department of Defense Computer Security Center (1985), *Department of Defense Password Management*, CSC-STD-002-95, Fort George Meade, MD.

9. Department of Justice (1991), *Code of Federal Regulations Title 28, Part 19*, National Archives and Records Administration, Washington, DC.

10. Department of Justice Order 2640.2B, *Automated Information Systems Security*, November 16, 1988.

11. Department of Justice Order 2640.3, *Unique Identification and Authentication of Users of Automated Information Systems*, March 30, 1990.

12. Federal Bureau of Investigation (1979), *The Identification Division of the FBI*, Washington, DC.

13. Federal Bureau of Investigation (1984), *The Science of Fingerprints: Classification and Uses*, Washington, DC.

14. Federal Bureau of Investigation (2004), *Disposition Submission via Machine Readable Data*, IAFIS-III-DOC-01008-2.1, June 30, 2006.

15. Federal Bureau of Investigation (2004), *Expungement Submission via Machine Readable Data*, IAFIS-III-DOC-01007-1.2, June 30, 2006.

NGI-486

16. Federal Bureau of Investigation (FBI), *AFIS Software Design Document, AFIS-DOC-02160-2.0, April 30, 2007.*

17. Federal Bureau of Investigation (FBI), *Best Practice Procedures for the Exchange of Latent Identification Services, Federal Bureau of Investigation, IAFIS – DOC– 03033 – 1.0*, July 26, 2005.

18. Federal Bureau of Investigation (FBI), *IAFIS Database Specification, IAFIS-DOC-02162-1.1*, May 3, 2007.

19. Federal Bureau of Investigation (FBI), *IAFIS Interface Control Document (ICD) IAFIS-DOC-05125-20.1*, April 30, 2007.

20. Federal Bureau of Investigation (FBI), *IAFIS Message Definition Database (MDD), IAFIS-DOC05125-19.0,* March 9, 2006.

21. Federal Bureau of Investigation (FBI), *IAFIS System Requirements Document (SRD, IAFIS-DOC - 01020 -11.2*, August 14, 2007.

22. Federal Bureau of Investigation (FBI), *IAFIS System Design Document, IAFIS-DOC-02098-5.5, August 1, 2007.*

23. Federal Bureau of Investigation (FBI), *IDWH Software Design Document*, IDWH-DOC-02041-6.5, August 10, 2007.

24. Federal Bureau of Investigation (FBI), *III Software Design Document (P-SPECS).*

25. Federal Bureau of Investigation (FBI), *Information Technology Life Cycle Management Directive (IT LCMD)* 2.0, November 19, 2004.

26. Federal Bureau of Investigation (FBI), *Machine Readable Data (MRD) Name Search Specifications*, IAFIS-DOC-01049-2.2, June 15, 2007.

27. Federal Bureau of Investigation (FBI), Integrated Automated Fingerprint Identification (IAFIS) System Target Architecture 2006.

28. Federal Bureau of Investigation (FBI), *Interstate Identification Index/National Fingerprint File (III/NFF) Operation and Technical Manual IAFIS-III-DOC-09034-1.0*, December 1, 2005.

29. Federal Bureau of Investigation (FBI), *ITN Software Design Document, ITN-DOC-02161-1.1*, April 23, 2007.

30. Federal Bureau of Investigation (FBI), *Manual of Investigative Operations and Guidelines (MIOG), Part II, Section 35 (FBI ADPT Security Manual),* July 26, 1995.

31. Federal Bureau of Investigation (FBI), *NCIC 2000 Operating Manual*, December 1999.

32. National Bureau of Standards (1985), NBS Special Publication 500-120, *Security of Personal Computer Systems: A Management Guide*, Washington, DC.

33. National Computer Security Center (1987), *Trusted Network Interpretation*, NCSC-TG-005, Version 1, Fort George Meade, MD.

34. National Technical Information Service (1975), FIPS PUB 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*, Washington, DC.

35. National Telecommunications and Information Systems Security Committee, National Telecommunications and Information Systems Security Policy, NTISSP No. 200, (1987), *National Policy on Controlled Access Protection*, Washington, DC.

36. Office of Management and Budget (1985), Circular No. A-130, Management of Federal Information Resources, Washington, DC.

37. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources,* February 20, 1996.

38. Office of Management and Budget (OMB), Bulletin No. 88-16, *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information*, Washington, DC, 1988.

39. Target Enterprise Architecture, EAPO-DOC-1077-1.1, August 2005.

40. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 65), Guideline for Automatic Data Processing (ADP) Risk Analysis, August 1, 1979.

41. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 73), *Guidelines for the Security of Computer Applications*, June 30, 1980.

42. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 87), *Guidelines for ADP Contingency Planning*, March 27, 1981.

43. U.S. Department of Commerce, Federal Information Processing Standards Publication (FIPS PUB 31), *Guidelines for Automatic Data Processing Physical Security and Risk Management*, June 1974.

44. U.S. Department of Commerce, *Federal Information Processing Standards Publication (FIPS PUB 112), Password Usage*, May 30, 1985.